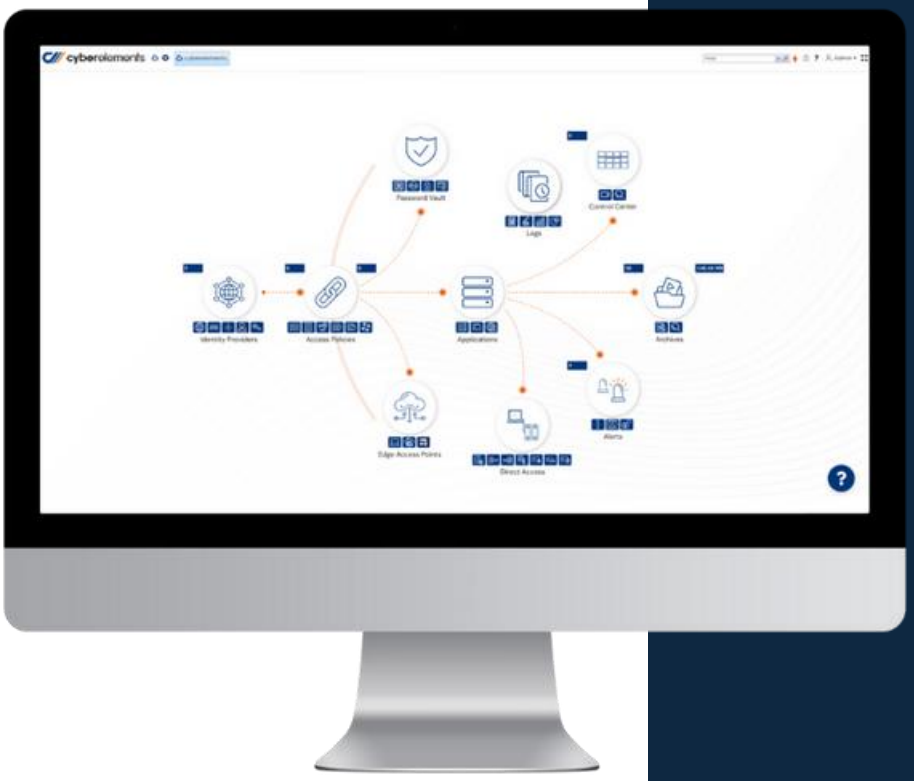
cyberelements Cleanroom

API cyberelements Cleanroom 4.6.1



www.systancia.com

Réf. :	FR_cyberelements-Cleanroom_MA-0003_API cyberelements Cleanroom_rev.1.05.docx
Version :	1.05
Produit :	**cyber**elements Cleanroom
Date :	2025-10-01

Objet :

Ce manuel couvre le fonctionnement de l'API de **cyber**elements Cleanroom 4.6.1.

TABLE DES MATIERES

1 Généralités

L'API de **cyber**elements Cleanroom 4.6.1 est une API REST. Elle est accessible sur l'adresse IP (HTTPS) du serveur Mediation Controller sur laquelle le site de **cyber**elements Cleanroom est configuré.

Les données envoyées et reçues par l'API sont au format JSON.

1.1 Mise en place de l'API

L'API doit être activée en modifiant le paramètre api/enabled dans le fichier /etc/ipdiva/care/djangosettings.ini présent sur le serveur Mediation Controller.

```
[api]
enabled = True
```

Suite à cela, il faut redémarrer le service *apache2* sur le serveur de Mediation Controller pour que le changement de paramètre soit appliqué.

1.2 Types de requêtes

Les méthodes de requêtes habituelles (GET, POST, DELETE, PUT, PATCH) sont utilisables avec cette API.

Toutefois, il faut savoir que :

- Une modification avec PUT remplace toujours l'intégralité des données de l'objet, sauf celles qui ne sont pas accessibles par l'API.
- Les URL se terminent toujours par le caractère slash.

Voici la liste des principales actions possibles :

Action	Exemple de requête
Récupérer une liste	GET publicapi/<ORGANISATION>/<TYPEOBJET>/
Récupérer un objet	GET publicapi/<ORGANISATION>/<TYPEOBJET>/<ID>/
Créer un objet	POST publicapi/<ORGANISATION>/<TYPEOBJET>/
Supprimer un objet	DELETE publicapi/<ORGANISATION>/<TYPEOBJET>/<ID>/
Modifier un objet	PUT publicapi/<ORGANISATION>/<TYPEOBJET>/<ID>/
Modifier un objet partiellement	PATCH publicapi/<ORGANISATION>/<TYPEOBJET>/<ID>/

Chaque section de ce document décrivant les éléments manipulables via cette API mentionnera les différentes URL utilisables, et spécifiera les méthodes disponibles. En l'absence telles précisions, les 5 méthodes de requêtes mentionnées ci-dessus sont utilisables pour les éléments en question.

1.3 Gestion des erreurs

Si l'appel a fonctionné, un code HTTP de succès est renvoyé. Il peut varier selon le type de requête. Par exemple, en cas de récupération d'un objet, le code 200 est reçu. En cas de suppression, le code 204 (No Content) est renvoyé.

En cas d'erreur, un code de retour HTTP d'erreur est renvoyé. Parmi les codes de retour possible, les plus courants sont :

- Le code 400 « Bad Request » est renvoyé si la requête ne respecte pas certaines contraintes, par exemple quand un paramètre obligatoire n'a pas été spécifié ou quand un champ ne pouvant pas être vide a été spécifié avec une valeur vide
- Le code 403 « Forbidden » est renvoyé si les informations d'authentification sont absentes ou invalides
- Le code 405 « Method Not Allowed » est renvoyé quand la méthode utilisée pour une requête n'est pas supportée pour cette URL. La plupart des requêtes que l'API REST supporte acceptent toutes les méthodes décrites dans la section Types de requêtes, mais ce n'est pas le cas pour toutes. Les sections de ce document décrivant comment manipuler les différents éléments de **cyber**elements Cleanroom font mention des exceptions à cette règle

Le format de la réponse à une requête varie selon le type d'erreur. En général, des données JSON sont envoyées avec une indication sur la cause de l'erreur. Cependant, dans certains cas, une erreur 500 peut être renvoyée. C'est par exemple le cas si l'opération demandée viole une contrainte d'intégrité de la base (doublons de valeurs censément uniques, etc…). Dans ces cas de figure, le détail de l'erreur ayant eu lieu est disponible dans les fichiers de logs du service *Apache2* sur le serveur Mediation Controller contacté (fichiers « /var/log/apache2/*_error.log »)

1.4 Présentation des concepts et exemples

Dans la suite de ce document, les éléments de **cyber**elements Cleanroom manipulables via l'API REST seront présentés un par un, chacun dans une section dédiée. Ces sections contiendront un certain nombre d'éléments, notamment :

- La liste des URL de l'API qui sont liées à l'élément en question.
- La liste des méthodes de requêtes (GET, POST, etc…) utilisable pour ces URL, si celle-ci diffère de la norme (voir Les types de requêtes)
- Une description du *Format des données* de l'élément décrit, sous la forme d'un encart contenant un exemple d'objet JSON représentant un élément type, suivi d'un tableau explicatif de chacune des propriétés de cet objet.
- Un ou plusieurs exemples d'envois de requêtes vers l'API REST, sous la forme d'un encart contenant un exemple écrit en code *Python* avec l'utilisation de la libraire *requests*.

2 API console d'administration

2.1 Authentification

Chaque appel à l'API nécessite d'être authentifié. L'authentification repose sur l'en-tête HTTP « Authorization », qui doit être spécifié dans toutes les requêtes vers l'API **cyber**elements Cleanroom. Cet en-tête doit contenir un jeton obtenu préalablement par un appel à une fonction dédiée à l'URL publicapi/api-auth.

Pour l'API de la console d'administration, les identifiants à spécifier sont ceux d'un administrateur du domaine local par défaut de l'organisation.

La configuration du domaine local par défaut de l'organisation s'applique : un trop grand nombre d'échecs d'authentification peut entrainer un verrouillage du compte utilisé, suivant ce qui a été configuré.

De plus, seule une configuration basique avec login/mot de passe peut être utilisée : si l'authentification par certificat est obligatoire sur ce domaine, l'accès à l'API REST est impossible. Il en va de même avec les autres fonctionnalités modifiant l'authentification, comme par exemple les OTP.

Exemple d'obtention du jeton :

```
import requests

r = requests.post('https://<mediation_server>/publicapi/api-auth', json={
    'login': 'admin',
    'password': 'secret',
    'org': 'organisation'
})
data = r.json()
try:
    id = data['id']
    print("Authentication succeeded")
except KeyError:
    print("Authentication failed")
    sys.exit(1)
```

L'appel doit contenir les paramètres suivants, en suivant la syntaxe JSON :

Paramètres	Description
login	Le nom de l'administrateur du domaine local de l'organisation.
password	Le mot de passe de l'administrateur du domaine local de l'organisation.
org	L'organisation cible des requêtes.

La réponse doit contenir un objet JSON contenant un champ « id » qui contient le jeton attendu. Ce jeton devra ensuite être placé dans l'en-tête « Authorization » pour les requêtes suivantes. Les exemples dans les sections suivantes incluront cet en-tête.

Si la réponse ne contient pas de champ « id », alors l'authentification a échoué.

2.2 Catégories

URL :

/publicapi/<ORGANISATION>/categories/

/publicapi/<ORGANISATION>/categories/<ID>/

/publicapi/<ORGANISATION>/categoriesbyname/< NAME>/

Format des données :

```
{
"name": "name",
"cat_id": 1
}
```

Paramètre	Description
name	Nom de la catégorie
cat_id	Identifiant de la catégorie (lecture seule)

Exemple de création :

```
data = {'name':'testapi'}

requests.post('https://<mediation_server>/publicapi/<org>/categories/', json=data,
headers={'Authorization': id})
```

Exemple de suppression :

```
requests.delete('https://<mediation_server>/publicapi/<org>/categories/1246/',head
ers={'Authorization':id})
```

2.3 Sites

URL :

/publicapi/<ORGANISATION>/sites/

/publicapi/<ORGANISATION>/sites/<ID>/

/publicapi/<ORGANISATION>/sitesbyname/<NAME>/

Format des données :

```
{
    "site_id": 1,
    "name": "site3",
    "description": "default site",
    "gateways": [
        {"gateway_name": "gw-name-1", "gateway_usage": "master"}
    ],
    "gateways_html5": ["gw-h5-name-1"]
}
```

Paramètre	Description
site_id	L'identifiant du site (lecture seule)
name	Nom du site
description	Texte descriptif du site
gateways	La liste des associations entre le site et l'ensemble des Edge Gateways. Chaque Edge Gateway de l'organisation est renseignée dans cette liste, avec son état au sein du site : • « master » si l'Edge Gateway est active • « slave » si l'Edge Gateway est passive • « nothing » si l'Edge Gateway est inutilisée
gateways_html5	La liste des noms des Edge Gateways HTML5 associées au site

Exemple de récupération de la liste des sites :

```
requests.get('https://<mediation_server>/publicapi/<org>/sites/',
headers={'Authorization':id})
```

Réponse :

```
[
    {
        "site_id":1,
        "name":"site3",
        "description":"default site",
        "gateways":[
            {"gateway_name": "gw-name-1","gateway_usage": "master"},
            {"gateway_name": "gw-name-2","gateway_usage": "nothing"}
        ],
        "gateways_html5": ["gw-h5-name-1", "gw-h5-name-2"]
    }
]
```

Exemple de modification d'un site :

```
data = {
    "name": "site_3",
    "description": "default site",
    "gateways": [
        {"gateway_name": "gw-name-3", "gateway_usage": "slave"}
    ]
    "gateway_html5": ["gw-h5-name-1"],
}

requests.patch('https://<mediation_server>/publicapi/<org>/sites/1/', json=data,
headers={"Authorization":id})
```

Note : Lors des créations et modifications *de sites, seules les Edge Gateways explicitement spécifiées dans le paramètre « gateways » sont impactées par la requête.* Les états des Edge Gateways non-spécifiées ne sont pas modifiés.

2.4 Edge Gateways

URL :

/publicapi/<ORGANISATION>/gateways/

/publicapi/<ORGANISATION>/gateways/<ID>/

/publicapi/<ORGANISATION>/gatewaysbyname/<NAME>/

Note : Il n'est pas possible de modifier des Edge Gateways via l'API, que ce soit via des requêtes PUT ou PATCH.

Format des données :


```
{
    "gateway_id": 1,
    "name": "test gateway",
    "description": "",
    "fqdn": "TEST_FQDN",
    "archive_path": "/var/lib/ipdiva/carerecord/archives",
    "ssh_archive_path": "/var/ipdiva/care/sshrecord",
    "status": {
        "online": true,
        "version": "8.9.1.1096"
    },
    "token": ""
}
```


Paramètre	Description
gateway_id	L'identifiant de l'Edge Gateway (lecture seule)
name	Nom de l'Edge Gateway. Doit être unique
description	Texte descriptif de l'Edge Gateway *Note : ce champ est actuellement obligatoire et ne peut pas être vide*
fqdn	FQDN (*Fully Qualified Domain Name*) de l'Edge Gateway
archive_path	Chemin vers l'emplacement des archives de sessions graphiques sur l'Edge Gateway (lecture seule)
ssh_archive_path	Chemin vers l'emplacement des archives de sessions SSH sur l'Edge Gateway(lecture seule)
status	Etat de l'Edge Gateway, indiquant si cette dernière est en ligne et quelle est son numéro de version (lecture seule)
token	Paramètre inutilisé (lecture seule)

Exemple de création :

```
data = {
    'name': 'test gateway',
    'fqdn': 'TEST_FQDN',
    'description': 'test description'
}

requests.post('https://<mediation_server>/publicapi/<org>/gateways/', json=data,
headers={"Authorization":id})
```

Note : Il n'est actuellement pas possible d'utiliser la fonctionnalité de création de jetons d'appairage via l'API REST.

2.5 Edge Gateways HTML5

URL :

/publicapi/<ORGANISATION>/html5gateways/

/publicapi/<ORGANISATION>/html5gateways/<ID>/

/publicapi/<ORGANISATION>/html5gatewaysbyname/<NAME>/

Format des données :


```
{
    "gateway_html5_id": 1,
    "name": "t3182-html5",
    "description": "",
    "url": "/HTML5_HTTP",
    "protocol": "http",
    "status": {
        "online": true,
        "version": "8.9.1.1096"
    },
    "token": ""
}
```


Paramètre	Description
gateway_html5_id	L'identifiant de l'Edge Gateway HTML5 (lecture seule)
name	Nom de l'Edge Gateway HTML5. Doit être unique
description	Texte descriptif de l'Edge Gateway HTML5 *Note : ce champ est actuellement obligatoire et ne peut pas être vide*
url	URL de l'Edge Gateway HTML5
protocol	Protocole à utiliser pour les communications avec l'Edge Gateway HTML5. Peut valoir « http » ou « websocket »
status	Etat de l'Edge Gateway, indiquant si cette dernière est en ligne et quelle est son numéro de version (lecture seule)
token	Paramètre inutilisé (lecture seule)

Exemple de création :

```
data = {
    "name": "test gw html5",
    "description": "test description",
    "url": "/HTML5",
    "protocol": "websocket"
}

requests.post('https://<mediation_server>/publicapi/<org>/html5gateways/',
json=data, headers={"Authorization":id})
```

2.6 Applications

Les applications sont classifiées par types d'application et en types de service.

Il existe deux types d'applications : « Application standard » et « Application privilégiée ». Chacun de ces deux types peut ensuite être décliné en plusieurs types de service.

Ces deux classifications déterminent le point d'entrée pour gérer les applications, de même que les paramètres acceptables et ceux requis par l'API pour leur manipulation. Cependant, toutes les applications reposent sur une base commune de paramètres, qui sont rassemblées dans un unique paramètre « resource ».

2.6.1 Paramètres communs

Toutes les applications reposant sur une base commune de paramètres, il est possible de lister les applications peu importe leur type de service, et récupérer tous ces paramètres communs.

URL :

/publicapi/<ORGANISATION>/resources/

/publicapi/<ORGANISATION>/resources/<ID>/

/publicapi/<ORGANISATION>/resourcesbyname/<NAME>/

Format des données :


```
{
   "resource_id": 2,
   "name": "test rds",
   "description": "",
   "category": "https://<mediation_server>/publicapi/<org>/categories/<id>/",
   "application_type": "priv",
   "service_type": "rdp",
   "restrictable": true,
   "assistance": false,
   "token_auth": 0,
   "ask_for_comment": false,
   "video_deletable": true,
   "video_storage_duration_days": null,
   "store_hash": false,
   "register_video": true,
   "enable_SSO": "sso-fixe",
   "aliases": ["alias_name_1"],
   "motd": "",
   "server": "1.2.3.4",
   "socket": 3389,
   "dynamic": false,
   "type": "",
   "ip_list": "",
   "ip_begin": null,
   "ip_end": null,
   "ip_mask": null,
   "mask": "",
   "setwindowtitle": false
```

```
}
```

Paramètre	Description
resource_id	Identifiant de l'application (lecture seule)
name	Nom de l'application. Doit être unique
description	Texte descriptif de l'application
category	Référence vers la catégorie à laquelle appartient l'application, sous la forme d'une URL de l'API REST
application_type	Type d'application de l'application. Valeurs possibles : « priv » et « std ». Bien que ce champ ne soit pas en lecture seule, Il est déconseillé de le modifier sur une application déjà existante car cela peut rendre l'application en question inutilisable
service_type	Type de service de l'application (lecture seule)
restrictable	Etat "peut être restreint" de l'application. Non-pertinent dans la majorité des cas d'usages
assistance	Paramètre obsolète
token_auth	Paramètre obsolète
ask_for_comment	Activation de la demande de commentaire à l'utilisateur. Si activé, lors du lancement de l'application, un commentaire sera demandé à l'utilisateur
video_deletable	Activation de la possibilité de supprimer manuellement les archives des sessions de cette application par les administrateurs, en passant par la console d'administration
video_storage_duration_days	Délai de conservation des archives de cette application, en nombre de jours. Une valeur vide désactive la suppression automatique des archives
store_hash	Activation du contrôle d'intégrité des vidéos lorsqu'elles sont lues
register_video	Activation de l'enregistrement vidéo des sessions de l'application. Désactiver cette option place l'application en mode d'enregistrement « événements uniquement », et désactive la génération d'une vidéo pour ses archives.

Paramètre	Description
	Pertinent uniquement pour les applications privilégiées graphiques
enable_SSO	Mode de SSO de l'application. Valeurs possibles : « sso », « no-sso », « askPassword » et « sso-fixe » • « sso » met le SSO de l'application en mode « Activé » • « no-sso » met le SSO de l'application en mode « Désactivé » • « askPassword » met le SSO de l'application en mode « Demander » • « sso-fixe » met le SSO de l'application en mode « Fixe » et permet alors l'association d'alias du coffre-fort à cette application (voir paramètre « aliases »)
aliases	Liste des noms des alias associés à cette application. Pertinent et obligatoire uniquement si le mode de SSO est « sso-fixe ». Si le coffre-fort est en mode *Keeper*, alors les noms des alias sont des UID Keeper. *Note : Il n'est actuellement pas possible d'associer un nouvel Alias Keeper avec une application via l'API Publique **cyber**elements Cleanroom*
motd	Message d'avertissement affiché à l'utilisateur lorsqu'il lance son application
dynamic	Activation du mode « application dynamique ». Une application dynamique ne cible pas une adresse unique, mais une collection d'adresses, demandant une saisie d'adresse spécifique par l'utilisateur au lancement de l'application
server	Serveur ciblé par l'application. Peut être une adresse IP ou un nom d'hôte. Pertinent et obligatoire uniquement pour les applications non-dynamiques
socket	Port du serveur ciblé par l'application. Pertinent uniquement pour les applications non-dynamiques
type	Type de restriction pour l'aspect "dynamique" de l'application, déterminant quelles adresses sont éligibles comme cibles lors du lancement de l'application. Peut prendre les valeurs suivantes :

Paramètre	Description
	• « ip_list » : l'application peut cibler les adresses explicitement mentionnées dans le paramètre « ip_list » • « ip_range » : l'application peut cibler les adresses IP comprises dans une plage d'adresse, définie via les paramètres « ip_begin » et « ip_end » • « ip_mask » : l'application peut cibler les adresses IP apparenant à un sous-réseau CIDR, défini via les paramètres « ip_mask » et « mask » Pertinent uniquement pour les applications dynamiques
ip_list	Liste exhaustive des adresses IP pouvant être ciblées par l'application. Pertinent et obligatoire uniquement pour les applications dynamiques avec un type de restriction « ip_list »
ip_begin	Première adresse IP de la plage des adresses IP autorisées comme cible de l'application. Pertinent et obligatoire uniquement pour les applications dynamiques avec un type de restriction « ip_range »
ip_end	Dernière adresse IP de la plage des adresses IP autorisées comme cible de l'application. Pertinent et obligatoire uniquement pour les applications dynamiques avec un type de restriction « ip_range »
ip_mask	Adresse IP du sous-réseau, utilisé conjointement avec le paramètre « mask » pour déterminer les adresses pouvant être ciblé par l'application. Pertinent et obligatoire uniquement pour les applications dynamiques avec un type de restriction « ip_mask »
mask	Masque de sous-réseau CIDR, utilisé conjointement avec le paramètre « ip_mask » pour déterminer les adresses pouvant être ciblé par l'application. Pertinent et obligatoire uniquement pour les applications dynamiques avec un type de restriction « ip_mask »
setwindowtitle	Activation de la réécriture du titre de la fenêtre de l'application, si elle est lancée en mode *fenêtré*. Si l'option est activée, le titre de la fenêtre de la session est remplacé par l'adresse ciblée par l'application (paramètre « server »). Pertinent uniquement pour les applications VNC et RDP avec un client *Windows*

2.6.2 Applications RDS privilégiées

URL :

/publicapi/<ORGANISATION>/rdpservices/

/publicapi/<ORGANISATION>/rdpservices/<ID>/

/publicapi/<ORGANISATION>/rdpservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications RDS, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :


```
{
    "service_id": 1,
    "resource": {},
    "colors_rdp": 24,
    "resolution": "fullscreen",
    "use_all_screen": false,
    "enable_CSSP": true,
    "redirect_clipboard": true,
    "plug_and_play": "",
    "redirect_audio_input": false,
    "mount_local_disk": false,
    "mount_local_printer": false,
    "enable_AUP": false,
    "connect_local_com_port": false,
    "console_mode": false,
    "remote_application": "",
    "launch_directory": "",
    "auth_domain": "",
    "ask_id": false,
    "noagent": false,
    "mstsc_arguments": "",
    "restricted_admin": false,
    "gw_on_workstation": false,
    "disable_kerberos": false,
    "kerberos_service_accounts": "",
    "custom_mstsc_options": "",
    "disable_mstsc_certificate_verification": false,
    "use_custom_app": false,
    "custom_app": "",
    "custom_app_arguments": "",
    "recorder_timeout_sec": 30,
    "broker_collection": "",
    "enable_recording_marker": true,
    "use_rds_broker": false
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
colors_rdp	Taille de la palette de couleurs à utiliser pour l'application, en nombre de bits. Peut valoir 16, 24 ou 32
resolution	Résolution à utiliser pour la fenêtre de l'application. Peut valoir « 640x480 », « 800x600 », « 1024x768 », « 1280x1024 », « 1600x1200 », « fullscreen » ou « dynamic »
use_all_screen	Utilisation des moniteurs pour la session à distance. Si l'option est activée, la session à distance pourra utiliser tous les moniteurs disponibles. Si elle est désactivée, un seul moniteur sera utilisé.
enable_CSSP	Utilisation du *Credential Security Support Provider* pour l'application
redirect_clipboard	Redirection du presse-papier du poste client vers la session RDP
plug_and_play	Liste des périphériques *Plug and Play* à utiliser depuis le client RDP du poste vers la session RDP
redirect_audio_input	Redirection des entrées audio du poste client vers la session RDP
mount_local_disk	Montage des disques du poste client sur le poste distant
mount_local_printer	Montage des imprimantes du poste client sur le poste distant
enable_AUP	Activation de la prise en charge du plugin *Applidis Universal Printing*
connect_local_com_port	Activation de la connexion des ports COM du poste client et du poste distant
console_mode	Activation du mode *Console* pour l'application

remote_application	Nom d'un exécutable présent sur le poste distant à exécuter automatiquement à l'ouverture d'une session
launch_directory	Répertoire de travail dans lequel l'exécutable spécifié dans « remote_application » se situe
auth_domain	Domaine d'authentification à utiliser pour l'authentification sur le poste distant. Si cette valeur est vide, le domaine d'authentification utilisé sera celui de l'alias ou du domaine **cyber**elements Cleanroom du compte utilisateur, en fonction du mode de SSO utilisé pour l'application
ask_id	Paramètre obsolète
noagent	Activation du mode *sans agent* pour cette application
mstsc_arguments	Arguments à transmettre à l'exécutable *mstsc.exe* lors de l'ouverture de la session distante. Pertinent uniquement pour les postes clients *Windows* utilisant *mstsc*
restricted_admin	Activation du mode *restrictedadmin* pour l'application. Ce mode interdit l'accès au poste distant pour les comptes n'ayant pas de droits administrateur sur ce dernier
gw_on_workstation	Activation de la fonctionnalité d'*Edge Gateway incorporée*. Inutilisable via l'API
disable_kerberos	Désactivation de *Kerberos* pour l'application. Pertinent uniquement si l'option « noagent » est activée
kerberos_service_accounts	Liste des comptes de service à utiliser pour récupérer le *TGT Kerberos*. Doit être spécifié en une seule chaine de caractère, où chaque nom de compte est séparé par une virgule. Pertinent uniquement si l'option « noagent » est activée et si l'option « disable_kerberos » est désactivée
custom_mstsc_options	Paramètres personnalisés du fichier RDP qui servira au lancement de l'application
disable_mstsc_certificate_verification	Désactivation de la vérification du certificat sur le poste client. Pertinent uniquement pour les postes clients *Windows* utilisant *mstsc*

use_custom_app	Activation de l'utilisation d'un programme client autre que *mstsc*. A utiliser conjointement avec les paramètres « custom_app » et « custom_app_arguments »
custom_app	Chemin vers l'exécutable du programme client à utiliser, présent sur le poste client. Pertinent uniquement si l'option « use_custom_app » est activée
custom_app_arguments	Arguments à transmettre au programme client lors du lancement de l'application. Pertinent uniquement si l'option « use_custom_app » est activée. Un certain nombre de variables peuvent être spécifiées dans ces arguments : « %IP% », « %PORT% », « %USER% », « %PASSWORD% », « %RESOURCENAME% » et « %SHELL% ».
recorder_timeout_sec	Délai d'interruption de la session **cyber**elements Cleanroom dans le cas où l'enregistreur ne se serait pas lancé, en secondes. Une valeur de 0 désactive l'interruption complètement
broker_collection	Collection de serveur du broker RDS. Pertinent uniquement si l'option « noagent » est activée et si les options « disable_kerberos » et « gw_on_workstation » sont désactivées
enable_recording_marker	Activation de l'affichage à l'utilisateur d'un indicateur d'enregistrement dans la fenêtre de l'application, si la session est effectivement enregistrée par **cyber**elements Cleanroom. Pertinent uniquement si l'option « noagent » est désactivée
use_rds_broker	Activation de l'utilisation d'un broker RDS. Pertinent uniquement si l'option « noagent » est désactivée

Exemple de création :

```
data = {
    'resource': {
        'name': 'test rds',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'video_deletable': True,
        'video_storage_duration_days': 365,
        'register_video': True,
        'enable_SSO': 'askPassword',
        'server': '1.2.3.4',
        'socket': 3389,
        'setwindowtitle': True,
    },
    'colors_rdp': 24,
    'resolution': 'fullscreen',
    'use_all_screen': True,
    'enable_CSSP': True,
    'redirect_clipboard': True,
    'mount_local_disk': True,
    'restricted_admin': True,
    'recorder_timeout_sec': 60,
    'enable_recording_marker': False
}

requests.post('https://<mediation_server>/publicapi/<org>/rdpservices/',
json=data, headers={"Authorization":id})
```

2.6.3 Applications RDP HTML5 privilégiées

URL :

/publicapi/<ORGANISATION>/html5rdpservices/

/publicapi/<ORGANISATION>/html5rdpservices/<ID>/

/publicapi/<ORGANISATION>/html5rdpservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications RDP HTML5, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :


```
{
    "service_id": 1,
    "resource": {},
    "resolution": "fullscreen",
    "resize_method": "zoom",
    "console_mode": false,
    "colors_html5": 32,
    "remote_application": "",
    "launch_directory": "",
    "auth_domain": "",
    "keyboard": "1036",
    "noagent": false,
    "security_mode": "any",
    "enable_wallpaper": false,
    "forcedomain": false,
    "redirect_html5_clipboard": true,
    "html_clipboard": false,
    "set_tab_title": false,
    "gw_on_workstation": false,
    "gateway_name": "",
    "gateway_zopeid": "",
    "disable_kerberos": false,
    "kerberos_service_accounts": "",
    "rdp_enable_file_transfer": false,
    "recorder_timeout_sec": 30,
    "broker_collection": "",
    "enable_recording_marker": true
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
resolution	Résolution à utiliser pour la fenêtre de l'application. Peut valoir « 640x480 », « 800x600 », « 1024x768 », « 1280x1024 », « 1600x1200 », « fullscreen » ou « dynamic »
resize_method	Méthode de redimensionnement de l'image. Peut valoir « zoom » ou « display update ». Pertinent uniquement si le paramètre « resolution » est défini à « fullscreen » ou « dynamic »
console_mode	Activation du mode *Console* pour l'application
colors_html5	Taille de la palette de couleurs à utiliser pour l'application, en nombre de bits. Peut valoir 16 ou 32. Si le paramètre « noagent » est désactivé, la valeur 8 est également acceptée
remote_application	Nom d'un exécutable présent sur le poste distant à exécuter automatiquement à l'ouverture d'une session
launch_directory	Répertoire de travail dans lequel l'exécutable spécifié dans « remote_application » se situe
auth_domain	Domaine d'authentification à utiliser pour l'authentification sur le poste distant. Pertinent uniquement si l'option « forcedomain » est désactivée
keyboard	Agencement de clavier à utiliser pour les sessions. La chaine représente la valeur base 10 du code LCID de la langue à utiliser. Les valeurs suivantes sont supportées : • « 1036 » : Français • « 1033 » : Anglais (US) • « 99998 » : Unicode AZERTY • « 99999 » : Unicode QWERTY • « 2055 » : Allemand (Suisse) • « 1031 » : Allemand (Allemagne) • « 4108 » : Français (Suisse) • « 2070 » : Portugais *Note : les valeurs « 99998 » et « 99999 » ne sont pas des codes LCID officiels, et sont utilisés par **cyber**elements Cleanroom pour des claviers génériques.*

Paramètre	Description
noagent	Activation du mode *sans agent* pour cette application
security_mode	Le mode de sécurité RDP. Si l'option « noagent » est activée, les valeurs « rdp » et « nla » sont acceptées. Si l'option « noagent » est désactivée, les valeurs « rdp », « nla », « tls » et « any » sont acceptées
enable_wallpaper	Activation du fond d'écran pour les sessions
forcedomain	Activation de l'utilisation du domaine du compte de connexion de l'utilisateur pour l'authentification auprès de la cible de l'application
redirect_html5_clipboard	Activation de la redirection du presse-papier du poste client vers la session. Cette redirection ne fonctionne que pour du contenu textuel
html_clipboard	Activation du presse-papier étendu, permettant la gestion de contenus textuels mis en forme
set_tab_title	Activation de la réécriture du titre des onglets des sessions. Si l'option est activée, le titre est remplacé par le nom de l'application (propriété « name » dans les paramètres communs)
gw_on_workstation	Activation de la fonctionnalité d'*Edge Gateway incorporée* pour l'application. A utiliser conjointement avec les paramètres « gateway_name » et « gateway_zopeid ». Incompatible avec le paramètre « broker_collection »
gateway_name	Nom de l' Edge Gateway incorporée. Doit correspondre au nom inscrit dans le certificat de cette dernière. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé
gateway_zopeid	ID Zope de l'Edge Gateway incorporée. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé
disable_kerberos	Désactivation de Kerberos pour l'application. Pertinent uniquement si l'option « noagent » est activée
kerberos_service_accounts	Liste des comptes de service à utiliser pour récupérer le TGT Kerberos. Doit être spécifié en une seule chaine de caractère, où chaque nom de compte est séparé par une virgule. Pertinent uniquement si l'option « noagent » est activée et si l'option « disable_kerberos » est désactivée
rdp_enable_file_transfer	Activation du transfert de fichier dans l'application

Paramètre	Description
recorder_timeout_sec	Délai d'interruption de la session **cyber**elements Cleanroom dans le cas où l'enregistreur ne se serait pas lancé, en secondes. Une valeur de 0 désactive l'interruption complètement
broker_collection	Collection de serveur du broker RDS. Pertinent uniquement si l'option « noagent » est activée et si les options « disable_kerberos » et « gw_on_workstation » sont désactivées
enable_recording_marker	Activation de l'affichage à l'utilisateur d'un indicateur d'enregistrement dans la fenêtre de l'application, si la session est effectivement enregistrée par **cyber**elements Cleanroom. Pertinent uniquement si l'option « noagent » est désactivée

Exemple de création :

```
data = {
    'resource': {
        'name': 'test rdp html5',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'video_deletable': True,
        'video_storage_duration_days': 365,
        'register_video': True,
        'enable_SSO': 'askPassword',
        'server': '1.2.3.4',
        'socket': 3389,
    },
    'resolution': 'fullscreen',
    'resize_method': 'zoom',
    'colors_html5': 32,
    'keyboard': '1036',
    'security_mode': 'tls',
    'enable_wallpaper': True,
    'redirect_html5_clipboard': True,
    'html_clipboard': True,
    'set_tab_title': True,
    'rdp_enable_file_transfer': True,
    'recorder_timeout_sec': 60,
    'enable_recording_marker': True
}

requests.post('https://<mediation_server>/publicapi/<org>/html5rdpservices/',
json=data, headers={"Authorization":id})
```

2.6.4 Applications SSH privilégiées

URL :

/publicapi/<ORGANISATION>/sshservices/

/publicapi/<ORGANISATION>/sshservices/<ID>/

/publicapi/<ORGANISATION>/sshservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications SSH, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :

```
{
    "auto_password": [
        {"pattern": "su -", "alias": "alias_name", "index": 0, "is_regex": false}
    ],
    "service_id": 1,
    "resource": {},
    "cmd_at_launch": "",
    "enable_file_transfer": false,
    "redirect_application": "",
    "redirect_params": "",
    "launch_app": false,
    "use_custom_app": false,
    "custom_app": "",
    "custom_app_arguments": "",
    "prompt_pattern": ""
}
```

Paramètre	Description
auto_password	Configurations d'injection de mots de passe, sous la forme d'une liste objets représentant chacun une configuration différente. Chaque configuration est composée des paramètres suivants : • « pattern » : motif déclencheur de l'injection, que **cyber**elements Cleanroom tente de détecter dans la session pour déclencher une injection de mot de passe • « alias » : nom de l'alias du coffre-fort **cyber**elements Cleanroom qui fournira le mot de passe à injecter. *Note : Dans le cas où le coffre-fort est en mode Keeper, ce nom doit être un UID Keeper* • « index » : numéro positif ou nul, représentant la priorité du motif déclencheur. Les motifs sont évaluées par ordre d'index croissants, et les numéros doivent être séquentiels (pas de doublons et pas de numéros manquants) *Note : un seul motif peut être déclenché par saisie. Si un motif est déclenché, tous les motifs avec une priorité moindre (donc avec un « index » supérieur) sont ignorés* • « is_regex » : option indiquant que le motif déclencheur est une expression régulière, et non pas une chaine de texte littérale
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
cmd_at_launch	Commande à exécuter dans la session SSH une fois la connexion établie. Pertinent uniquement si l'option « enable_file_transfert » est désactivée
enable_file_transfer	Activation du mode *Transfert de fichiers*. Si cette option est activée, l'application servira à établir une connexion SFTP au lieu d'une connexion SSH
redirect_application	Paramètre obsolète
redirect_params	Paramètre obsolète

launch_app	Paramètre obsolète
use_custom_app	Activation de l'utilisation d'un programme client spécifique pour le lancement de l'application. A utiliser conjointement avec les paramètres « custom_app » et « custom_app_arguments »
custom_app	Chemin vers l'exécutable du programme client à utiliser, présent sur le poste client. Pertinent uniquement si l'option « use_custom_app » est activée
custom_app_arguments	Arguments à transmettre au programme client lors du lancement de l'application. Pertinent uniquement si l'option « use_custom_app » est activée Un certain nombre de variables peuvent être spécifiées dans ces arguments : « %IP% », « %PORT% », « %USER% », « %PASSWORD% », « %RESOURCENAME% » et « %SHELL% »
prompt_pattern	Motif de l'invite de commande de la session SSH

Exemple de création :

```
data = {
    'resource': {
        'name': 'test ssh',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'enable_SSO': 'sso-fixe',
        'aliases': ['user_alias_name'],
        'server': '1.2.3.4',
        'socket': 22,
    },
    "auto_password": [
        {"pattern": "^su$", "alias": "root_alias_name", "index": 0, "is_regex":
True},
        {"pattern": "sudo -s", "alias": "root_alias_name", "index": 1, "is_regex":
False},
    ],
}

requests.post('https://<mediation_server>/publicapi/<org>/sshservices/',
json=data, headers={"Authorization":id})
```

Exemple de mise à jour des configurations d'injections de mot de passes SSH avec le coffre-fort en mode *Keeper* :

```
data = {
    "auto_password": [
        {'pattern': '^su$', 'alias': 'GeiUk2qWMdEodi-6SfU3Pw', 'index': 0,
'is_regex': True},
        {'pattern': 'sudo -s', 'alias': 'Qj93wfPHm2LedB7cFjKdzg', 'index': 1,
'is_regex': False},
    ]
}

requests.patch('https://<mediation_server>/publicapi/<org>/sshservices/1/',
json=data, headers={"Authorization": id})
```

2.6.5 Applications SSH HTML5 privilégiées

URL :

/publicapi/<ORGANISATION>/html5sshservices/

/publicapi/<ORGANISATION>/html5sshservices/<ID>/

/publicapi/<ORGANISATION>/html5sshservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications SSH HTML5, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :

```
{
    "auto_password": [],
    "service_id": 1,
    "resource": {},
    "cmd_at_launch": "",
    "term_type": "linux",
    "enable_file_transfer": false,
    "redirect_html5_clipboard": true,
    "backspace_key": 127,
    "set_tab_title": false,
    "prompt_pattern": ""
}
```

Paramètre	Description
auto_password	Configurations d'injection de mots de passe, sous la forme d'une liste objets représentant chacun une configuration différente. Chaque configuration est composée des paramètres suivants : • « pattern » : motif déclencheur de l'injection, que **cyber**elements Cleanroom tente de détecter dans la session pour déclencher une injection de mot de passe • « alias » : nom de l'alias du coffre-fort **cyber**elements Cleanroom qui fournira le mot de passe à injecter. *Note : Dans le cas où le coffre-fort est en mode Keeper, ce nom doit être un UID Keeper* • « index » : numéro positif ou nul, représentant la priorité du motif déclencheur. Les motifs sont évaluées par ordre d'index croissants, et les

	numéros doivent être séquentiels (pas de doublons et pas de numéros manquants) *Note : un seul motif peut être déclenché par saisie. Si un motif est déclenché, tous les motifs avec une priorité moindre (donc avec un « index » supérieur) sont ignorés* • « is_regex » : option indiquant que le motif déclencheur est une expression régulière, et non pas une chaine de texte littérale
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
cmd_at_launch	Commande à exécuter dans la session SSH une fois la connexion établie. Pertinent uniquement si l'option « enable_file_transfert » est désactivée
term_type	Type de terminal à simuler pour les sessions utilisant cette application
enable_file_transfer	Activation du mode *Transfert de fichiers*. Si cette option est activée, l'application servira à établir une connexion SFTP au lieu d'une connexion SSH
redirect_html5_clipboard	Activation de la redirection du presse-papier du poste client vers la session. Cette redirection ne fonctionne que pour du contenu textuel
backspace_key	Entier représentant le code ASCII du caractère de retour arrière à considérer pour les sessions utilisant cette application. Les valeurs 8 (caractère « backspace ») et 127 (caractère « delete ») sont supportées
set_tab_title	Activation de la réécriture du titre des onglets des sessions. Si l'option est activée, le titre est remplacé par le nom de l'application (propriété « name » dans les paramètres communs)
prompt_pattern	Motif de l'invite de commande de la session SSH

Exemple de création :

```
data = {
    'resource': {
        'name': 'test h5 ssh',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'enable_SSO': 'askPassword',
        'server': '1.2.3.4',
        'socket': 22,
    },
    "auto_password": [],
    'term_type': 'linux',
    'backspace_key': 127,
    'set_tab_title': True,
}

requests.post('https://<mediation_server>/publicapi/<org>/html5sshservices/',
json=data, headers={"Authorization":id})
```

2.6.6 Applications VNC privilégiées

URL :

/publicapi/<ORGANISATION>/vncservices/

/publicapi/<ORGANISATION>/vncservices/<ID>/

/publicapi/<ORGANISATION>/vncservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications VNC, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :

```
{
    "service_id": 1,
    "resource": {},
    "custom_mstsc_options": "",
    "disable_mstsc_certificate_verification": false,
    "use_custom_app": false,
    "custom_app": "",
    "custom_app_arguments": "",
    "gw_on_workstation": false,
    "gateway_name": "",
    "gateway_zopeid": ""
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
custom_mstsc_options	Paramètres personnalisés du fichier RDP qui servira au lancement de l'application
disable_mstsc_certificate_verification	Désactivation de la vérification du certificat sur le poste client. Pertinent uniquement pour les postes clients *Windows* utilisant *mstsc*
use_custom_app	Activation de l'utilisation d'un programme client autre que *mstsc*. A utiliser conjointement avec les paramètres « custom_app » et « custom_app_arguments »

custom_app	Chemin vers l'exécutable du programme client à utiliser, présent sur le poste client. Pertinent uniquement si l'option « use_custom_app » est activée
custom_app_arguments	Arguments à transmettre au programme client lors du lancement de l'application. Pertinent uniquement si l'option « use_custom_app » est activée Un certain nombre de variables peuvent être spécifiées dans ces arguments : « %IP% », « %PORT% », « %USER% », « %PASSWORD% », « %RESOURCENAME% » et « %SHELL% »
gw_on_workstation	Activation de la fonctionnalité d'*Edge Gateway incorporée* pour l'application. A utiliser conjointement avec les paramètres « gateway_name » et « gateway_zopeid ». Incompatible avec le paramètre « broker_collection »
gateway_name	Nom de l'Edge Gateway incorporée. Doit correspondre au nom inscrit dans le certificat de cette dernière. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé
gateway_zopeid	ID Zope de l'Edge Gateway incorporée. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé

Exemple de création :

```
data = {
    'resource': {
        'name': 'test vnc',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'enable_SSO': 'no-sso',
        'server': '1.2.3.4',
        'socket': 5900,
    },
    'custom_mstsc_options': '',
    'disable_mstsc_certificate_verification': True,
    'use_custom_app': False,
    'gw_on_workstation': False,
}

requests.post('https://<mediation_server>/publicapi/<org>/vncservices/',
json=data, headers={"Authorization":id})
```

2.6.7 Applications VNC HTML5 privilégiées

URL :

/publicapi/<ORGANISATION>/html5vncservices/

/publicapi/<ORGANISATION>/html5vncservices/<ID>/

/publicapi/<ORGANISATION>/html5vncservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications VNC HTML5, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :

```
{
    "service_id": 1,
    "resource": {},
    "redirect_html5_clipboard": true,
    "set_tab_title": false,
    "gw_on_workstation": false,
    "gateway_name": "",
    "gateway_zopeid": ""
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
redirect_html5_clipboard	Activation de la redirection du presse-papier du poste client vers la session. Cette redirection ne fonctionne que pour du contenu textuel
set_tab_title	Activation de la réécriture du titre des onglets des sessions. Si l'option est activée, le titre est remplacé par le nom de l'application (propriété « name » dans les paramètres communs)
gw_on_workstation	Activation de la fonctionnalité d'*Edge Gateway incorporée* pour l'application. A utiliser conjointement avec les paramètres « gateway_name » et « gateway_zopeid ». Incompatible avec le paramètre « broker_collection »

gateway_name	Nom de l'Edge Gateway incorporée. Doit correspondre au nom inscrit dans le certificat de cette dernière. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé
gateway_zopeid	ID Zope de l'Edge Gateway incorporée. Pertinent et obligatoire uniquement si « gw_on_workstation » est activé

Exemple de création :

```
data = {
    'resource': {
        'name': 'test h5 vnc',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'enable_SSO': 'no-sso',
        'server': '1.2.3.4',
        'socket': 5900,
    },
    'set_tab_title': True,
    'gw_on_workstation': False,
}

requests.post('https://<mediation_server>/publicapi/<org>/html5vncservices/',
json=data, headers={"Authorization":id})
```

2.6.8 Applications Web privilégiées

URL :

/publicapi/<ORGANISATION>/webrecordservices/

/publicapi/<ORGANISATION>/ webrecordservices /<ID>/

/publicapi/<ORGANISATION>/ webrecordservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications Web, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :


```
{
    "service_id": 1,
    "resource": {},
    "secure_connection": true,
    "url": "",
    "target_server": "www.example.com",
    "enable_recording_marker": true,
    "sso_form_mode": 2,
    "sso_login_field": "",
    "sso_password_field": "",
    "sso_form_data": "",
    "sso_advanced_data_enabled": false,
    "sso_advanced_data": "",
    "auth_mode": 2,
    "sso_type": "classic",
    "sso_url": "",
    "html_sso": false,
    "use_form_action_attr": false,
    "additionnal_networks": false,
    "injection_conf": ""
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « priv »
secure_connection	Activation des connexions sécurisées avec le serveur Web distant. Si l'option est activée, les communications seront faites avec le protocole HTTPS. Si elle est désactivée, le protocole HTTP sera utilisé
url	Chemin d'accès à l'application Web distante
target_server	Hôte Web distant ciblé par l'application. Peut être un nom d'hôte ou une adresse IP, optionnellement accompagnée d'un numéro de port. Ce champ remplace la valeur du paramètre commun « server » (voir Paramètres communs)
enable_recording_marker	Activation de l'affichage à l'utilisateur d'un indicateur d'enregistrement dans la fenêtre de l'application, si la session est effectivement enregistrée par **cyber**elements Cleanroom. Pertinent uniquement si l'option « noagent » est désactivée
sso_form_mode	Mode du formulaire, dans le cadre d'un SSO sur formulaires HTML. Pertinent uniquement si le paramètre « html_sso » est activé et si « sso_type » vaut « classic » ou « preload »
sso_login_field	Nom du champ du formulaire HTML d'authentification devant contenir le nom du compte de l'utilisateur. Pertinent uniquement si le paramètre « html_sso » est activé, si « sso_advanced_data_enabled » est désactivé et si « sso_type » vaut « classic » ou « preload »
sso_password_field	Nom du champ du formulaire HTML d'authentification devant contenir le mot de passe du compte de l'utilisateur. Pertinent uniquement si le paramètre « html_sso » est activé, si « sso_advanced_data_enabled » est désactivé et si « sso_type » vaut « classic » ou « preload »
sso_form_data	Paramètres additionnels pour le formulaire HTML d'authentification. Pertinent uniquement si le paramètre « html_sso » est activé, si

	« sso_advanced_data_enabled » est désactivé et si « sso_type » vaut « classic » ou « preload »
sso_advanced_data_enabled	Activation du mode paramétrage avancé, permttant de spécifier les données du formulaire HTML en un seul paramètre « sso_advanced_data ». Rend inutile les paramètres « sso_login_field », « sso_password_field » et « sso_form_data »
sso_advanced_data	Paramétrage avancé pour le formulaire HTML d'authentification. Pertinent uniquement si le paramètre « html_sso » et « sso_advanced_data_enabled » sont activés et si « sso_type » vaut « classic » ou « preload »
auth_mode	Type d'authentification. Peut prendre l'une des valeurs suivantes : • 1 pour « Authentification basique » • 2 pour « Détection automatique »
sso_type	Type de SSO sur un formulaire HTML Classique. Peut prendre l'une des valeurs suivantes : • « classic » pour le mode « Classique » • « preload » pour le mode « Préchargement de formulaire » • « preauth » pour le mode « Pré-authentification » • « inject » pour le mode « Injection » Pertinent uniquement si le paramètre « html_sso » est activé *Note : il n'est actuellement pas possible de configurer un type de sso « preauth » fonctionnel via l'API REST.*
sso_url	Chemin d'accès vers le formulaire HTML d'authentification à pré-charger. Pertinent uniquement si le paramètre « html_sso » est activé et si « sso_type » vaut « preload »
html_sso	Activation du mode de SSO sur les formulaires HTML classiques. Permet l'utilisation du paramètre « sso_type »
use_form_action_attr	Activation de la détection automatique du chemin d'accès vers la page Web distante en se basant sur l'attribut « action » du formulaire HTML. Rend inopérant le paramètre « url »
additionnal_networks	Autorisation des réseaux supplémentaires.

	Note : il n'est actuellement pas possible de configurer ces réseaux supplémentaires via l'API REST.
injection_conf	Configuration d'injection, telle que générée par le plugin navigateur prévu à cet effet. Pertinent uniquement si le paramètre « html_sso » est activé et si « sso_type » vaut « inject »

Exemple de création :

```
data = {
    'resource': {
        'name': 'test web sso preload',
        'description': '',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'priv',
        'enable_SSO': 'sso',
    },
    'secure_connection': True,
    'url': '',
    'target_server': 'www.example.com',
    'enable_recording_marker': True,
    'sso_form_mode': 2,
    'sso_login_field': 'user_login',
    'sso_password_field': 'user_pwd',
    'sso_type': 'preload',
    'sso_url': 'api/authform.html',
    'html_sso': True,
    'use_form_action_attr': True,
    "sso_form_data": "",
    "sso_advanced_data": "",
    "auth_mode": 2,
}

requests.post('https://<mediation_server>/publicapi/<org>/webrecordservices/',
json=data, headers={"Authorization":id})
```

2.6.9 Applications Web standards

URL :

/publicapi/<ORGANISATION>/standardwebrecordservices/

/publicapi/<ORGANISATION>/standardwebrecordservices/<ID>/

/publicapi/<ORGANISATION>/standardwebrecordservicesbyname/<NAME>/

Le format des données et les paramètres acceptés sont strictement identiques aux applications Web privilégiées, à ceci près que le « application_type » doit être défini comme « std » et non « priv ».

2.6.10 Applications tunnel générique standards

URL :

/publicapi/<ORGANISATION>/portforwardservices/

/publicapi/<ORGANISATION>/portforwardservices/<ID>/

/publicapi/<ORGANISATION>/portforwardservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications Tunnel Générique, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données de l'application :

```
{
    "service_id": 1,
    "resource": {},
    "redirect_application": "",
    "redirect_params": "",
    "launch_app": false,
    "alert_user": true,
    "redirect_html_sso": false,
    "launch_web_app": false,
    "enable_url_rewriting": false,
    "preserve_host": false,
    "avoid_windows_auth": false,
    "url_app": "",
    "redirect_sso_login": "",
    "redirect_sso_password": "",
    "redirect_sso_extra": "",
    "redirect_sso_method": 2,
    "default_port": 0,
    "redirections": [
        {
            "id_for_resource": 0,
            "redirect_protocol": "ssh",
            "remote_server": "1.1.1.1",
            "remote_port": 22,
            "local_server": "127.0.0.1",
            "desired_local_port": 0
        }
    ]
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « std »
redirect_application	Exécutable redirigé à exécuter lors du lancement de l'application. Pertinent uniquement si le paramètre « launch_app » est activé
redirect_params	Paramètres pour l'exécutable redirigé. Pertinent uniquement si le paramètre « launch_app » est activé
launch_app	Activation de l'exécution automatique d'un exécutable redirigé. Permet également l'utilisation d'un mode de SSO avec cette application (voir Paramètres communs). Il est déconseillé d'utiliser cette option si « alert_user » ou « launch_web_app » est activé
alert_user	Activation de la notification prévenant l'utilisateur lorsque la connexion est établie. Il est déconseillé d'utiliser cette option si « launch_app » ou « launch_web_app » est activé
redirect_html_sso	Activation du mode de SSO sur les formulaires HTML classiques. Pertinent uniquement si « launch_web_app » est activé
launch_web_app	Activation du lancement automatique via navigateur Web. Permet également l'utilisation d'un mode de SSO avec cette application (voir Paramètres communs). Il est déconseillé d'utiliser cette option si « launch_app » ou « alert_user » est activé. Pertinent uniquement si au moins une redirection de port spécifiée dans le paramètre « redirections » est configuré avec l'un des protocoles suivants : « http », « https » ou « lotus-web »
enable_url_rewriting	Activation de la réécriture d'URL. Pertinent uniquement si au moins une redirection de port spécifiée dans le paramètre « redirections » est configuré avec l'un des protocoles suivants : « http », « https » ou « lotus-web »
preserve_host	Activation de la préservation de l'en-tête *Host*. Pertinent uniquement si au moins une redirection de port spécifiée dans le paramètre « redirections » est

	configuré avec l'un des protocoles suivants : « http », « https » ou « lotus-web »
avoid_windows_auth	Activation de la parade d'authentification Windows. Pertinent uniquement si au moins une redirection de port spécifiée dans le paramètre « redirections » est configuré avec l'un des protocoles suivants : « http », « https » ou « lotus-web »
url_app	URL à lancer automatiquement. Pertinent uniquement si le paramètre « launch_web_app » est activé
redirect_sso_login	Nom du champ du formulaire HTML d'authentification devant contenir le nom du compte de l'utilisateur. Pertinent uniquement si le paramètre « redirect_html_sso » est activé
redirect_sso_password	Nom du champ du formulaire HTML d'authentification devant contenir le mot de passe du compte de l'utilisateur. Pertinent uniquement si le paramètre « redirect_html_sso » est activé
redirect_sso_extra	Paramètres additionnels pour le formulaire HTML d'authentification. Pertinent uniquement si le paramètre « redirect_html_sso » est activé
redirect_sso_method	Méthode à utiliser pour la soumission du formulaire d'authentification HTML. Peut prendre l'une des valeurs suivantes : • 1 pour la méthode « GET » • 2 pour la méthode « POST »
default_port	Port distant par défaut pour les redirections dans le cas où l'application tunnel générique est *dynamique* (voir Paramètres communs). *Note : il n'est pas possible de configurer une application tunnel générique standard en mode dynamique via l'API REST*
redirections	Liste des configurations de cette application. Chaque redirection doit respecter un format spécifique, décrit ci-après

Format des données des redirections :

```
{
    "id_for_resource": 0,
    "redirect_protocol": "ssh",
    "remote_server": "1.1.1.1",
    "remote_port": 22,
    "local_server": "127.0.0.1",
    "desired_local_port": 0
}
```

Paramètre	Description
id_for_resource	Identifiant de la redirection (doit être unique au sein de l'application)
redirect_protocol	Protocole à rediriger. Peut prendre l'une des valeurs suivantes : • « ftp » • « http » • « https » • « ica » • « imap » • « impas » • « mapi » • « notes » • « pop » • « pops » • « prox-funk » • « proxy-web » • « rlogin » • « smtp » • « socks » • « ssh » • « telnet » • « tse » • « selligent » • « lotus-web » • « other-tcp » • « other-udp »

remote_server	Adresse cible de la redirection
remote_port	Port cible de la redirection
local_server	Adresse source de la redirection
desired_local_port	Port source de la redirection

Notes :

- *Il n'est pas possible de configurer une application tunnel générique standard en mode dynamique via l'API REST*
- *Les paramétrages de SSO ne sont pertinents que si l'une des options de lancement automatique est activée (« launch_app » ou « launch_web_app »)*

Exemple de création d'une application sans lancement automatique :

```
data = {
    'resource': {
        'name': 'test port forward',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'std',
        'server': '',
        'socket': 0,
    },
    'alert_user': True,
    'redirections': [
        {
            'id_for_resource': 0,
            'redirect_protocol': 'ssh',
            'remote_server': '1.1.1.1',
            'remote_port': 22,
            'local_server': '127.0.0.1',
            'desired_local_port': 50022
        },
        {
            'id_for_resource': 1,
            'redirect_protocol': 'ssh',
            'remote_server': '2.2.2.2',
            'remote_port': 22,
            'local_server': '127.0.0.1',
            'desired_local_port': 50023
        }
    ]
}

requests.post('https://<mediation_server>/publicapi/<org>/portforwardservices/',
json=data, headers={"Authorization":id})
```

Exemple de création d'une application avec un lancement automatique dans le navigateur :

```
data = {
    'resource': {
        'name': 'test port forward',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'std',
        'enable_SSO': 'sso-fixe',
        'aliases': ['example.com admin']
    },
    'redirect_html_sso': True,
    'launch_web_app': True,
    'enable_url_rewriting': False,
    'preserve_host': False,
    'avoid_windows_auth': True,
    'url_app': 'path/to/index.html',
    'redirect_sso_login': 'user_login',
    'redirect_sso_password': 'user_pwd',
    'redirect_sso_extra': '',
    'redirect_sso_method': 2,
    'redirections': [
        {
            'id_for_resource': 0,
            'redirect_protocol': 'https',
            'remote_server': 'example.com',
            'remote_port': 443,
            'local_server': '127.0.0.1',
            'desired_local_port': 443
        }
    ]
}

requests.post('https://<mediation_server>/publicapi/<org>/portforwardservices/',
json=data, headers={"Authorization":id})
```

2.6.11 Applications VPN standards

URL :

/publicapi/<ORGANISATION>/vpnservices/

/publicapi/<ORGANISATION>/vpnservices/<ID>/

/publicapi/<ORGANISATION>/vpnservicesbyname/<NAME>/

Note : l'identifiant à spécifier pour les URL est le « service_id » présent dans les données spécifiques aux applications VPN, tandis que le nom attendu est celui trouvable dans le paramètre « name » des données communes des applications*.*

Format des données :


```
{
    "service_id": 1,
    "resource": {},
    "display_gui": true,
    "mode": "routing",
    "protocol": "tcp",
    "network": "10.10.0.0",
    "netmask": "255.255.255.0",
    "network_begin": null,
    "netmask_begin": null,
    "network_end": null,
    "netmask_end": null,
    "ip_policy": "dhcp",
    "dns_suffix": "",
    "fulltunnel_enabled": false,
    "routes": [
        {
            "ip": "1.1.1.0",
            "netmask": "255.255.255.0"
        },
        {
            "ip": "2.2.2.0",
            "netmask": "255.255.255.0"
        }
    ],
    "allowed_networks_ip": [
        {
            "ip": "*"
        }
    ],
    "forbidden_networks": [
        {
            "ip": "1.1.1.1"
        }
    ],
    "allowed_networks_ip_range": [
        {
            "begin_ip": "1.1.1.1",
```

```
            "end_ip": "2.2.2.2"
        }
    ],
    "allowed_networks_mask": [
        {
            "ip": "1.1.1.0",
            "netmask": "255.255.255.0"
        },
        {
            "ip": "1.1.1.0",
            "netmask": "24"
        }
    ],
    "dns_servers": [
        {
            "dns_server": "lan.local"
        }
    ]
}
```

Paramètre	Description
service_id	Identifiant du service (lecture seule)
resource	Objet contenant les paramètres communs de l'application. Parmi ces paramètres, le « application_type » doit être placé à « std »
display_gui	Activation du retour visuel à l'utilisateur concernant l'état du VPN
mode	Mode de l'application VPN. Seule la valeur « routing » est supportée
protocol	Protocole à utiliser pour les communications. Peut prendre la valeur « tcp » ou « udp »
network	Adresse IP du réseau du VPN, à spécifier conjointement avec le paramètre « netmask »
netmask	Masque de sous-réseau en notation décimale, à spécifier conjointement avec le paramètre « network »
network_begin	Paramètre inutilisé
netmask_begin	Paramètre inutilisé
network_end	Paramètre inutilisé

netmask_end	Paramètre inutilisé
ip_policy	Stratégie d'allocation des adresses IP des utilisateurs pour l'application. Seule la valeur « dhcp » est supportée
dns_suffix	Suffixe DNS du VPN
fulltunnel_enabled	Activation du mode « full tunneling », permettant de rediriger tout le flux réseau vers le tunnel VPN. Rend le paramètre « routes » inutile
routes	Listes des routes qui seront mises en place sur le poste de l'utilisateur, lui permettant d'atteindre les différents segments réseau du site distant. Chaque route est un objet avec deux clés « IP » et « netmask », respectivement l'adresse et le masque du sous-réseau. Le masque ne peut être spécifié qu'en notation décimale. Pertinent uniquement si l'option « fulltunnel_enabled » est désactivée
allowed_networks_ip	Liste des *réseaux autorisés* de type « IP » pour le VPN. Chaque élément de la liste est un objet avec une clé « ip » ayant pour valeur soit l'adresse à autoriser, soit le *wildcard* « * »
forbidden_networks	Liste des *réseaux autorisés* de type « IP interdite » pour le VPN. Chaque élément de la liste doit respecter la même structure que pour les éléments spécifiables pour « allowed_networks_ip »
allowed_networks_ip_range	Liste des *réseaux autorisés* de type « Plage d'IP » pour le VPN. Chaque élément de la liste est un objet avec deux clés « begin_ip » et « end_ip » dont les valeurs sont des adresses IP, respectivement la première et la dernière de la plage
allowed_networks_mask	Liste des *réseaux autorisés* de type « Sous réseau » pour le VPN. Chaque élément de la liste est un objet avec deux clés « ip » et « netmask », respectivement l'adresse et le masque du sous-réseau. Le masque peut être spécifié en notation décimale ou CIDR
dns_servers	Liste des serveurs DNS à utiliser pour les résolutions de noms de domaines. Chaque élément de la liste est un objet avec une clé « dns_server » dont la valeur peut être une adresse IP ou un nom d'hôte

Exemple de création :

```
data = {
    'resource': {
        'name': 'test vpn',
        'category': 'https://<mediation_server>/publicapi/<org>/categories/<id>/',
        'application_type': 'std',
    },
    'display_gui': False,
    'protocol': 'tcp',
    'network': '10.10.0.0',
    'netmask': '255.255.255.0',
    'dns_suffix': 'local',
    'fulltunnel_enabled': False,
    'routes': [{'ip': '10.10.1.0', 'netmask': '255.255.255.0'}, {'ip':
'10.10.2.0', 'netmask': '255.255.255.0'}],
    'allowed_networks_ip': [{'ip': '*'}],
    'forbidden_networks': [],
    'allowed_networks_ip_range': [],
    'allowed_networks_mask': [],
    'dns_servers': [{'dns_server': 'lan.local'}]
}

requests.post('https://<mediation_server>/publicapi/<org>/vpnservices/',
json=data, headers={"Authorization":id})
```

2.7 Contrats d'accès

2.7.1 Informations de base

Les données de contrats d'accès correspondent aux données disponibles dans la console d'administration. Les sites, catégories et applications associées sont indiquées sous forme de listes contenant des URL vers les objets de l'API associés, dans les champs « sites », « categories » et « resources ».

Il n'y a cependant pas les informations liées aux groupes d'utilisateurs, qui sont gérés différemment (voir Gestion des groupes et domaines dans les contrats).

URL :

publicapi/<ORGANISATION>/accessprofiles/

publicapi/<ORGANISATION>/accessprofiles/<ID>/

publicapi/<ORGANISATION>/accessprofilesbyname/<NAME>/

Format des données :

```
{
    "access_profile_id": 1,
    "name": "test access profile",
    "description": "",
    "resources": [
        "https://<mediation_server>/publicapi/<org>/resources/524/"
    ],
    "categories": [
        "https://<mediation_server>/publicapi/<org>/categories/1/",
        "https://<mediation_server>/publicapi/<org>/categories/2/"
    ],
    "sites": [
        "https://<mediation_server>/publicapi/<org>/sites/2/"
    ]
}
```

Paramètre	Description
access_profile_id	Identifiant du contrat d'accès (lecture seule)
name	Nom du contrat d'accès. Doit être unique
description	Texte descriptif du contrat d'accès
resources	Liste des URL de l'API REST référençant les applications explicitement concernées par ce contrat d'accès. Une application appartenant à une catégorie spécifiée dans le paramètre « categories » n'a pas besoin d'être spécifiée dans « resources »
categories	Liste des URL de l'API REST référençant les catégories d'applications explicitement concernées par ce contrat d'accès. Toutes les applications appartenant à ces catégories sont indirectement concernées par le contrat d'accès. Ces applications n'ont donc pas besoin d'être spécifiées dans le paramètre « resources »
sites	Liste des URL de l'API REST référençant les sites associés à ce contrat d'accès, définissant quelles Edge Gateways et Edge Gateways HTML5 seront disponibles pour ces accès.

Exemple de création :

```
data = {
    'name': 'test access profile',
    'description': '',
    'resources': [],
    'categories': ['https://<mediation_server>/publicapi/<org>/categories/1/'],
    'sites': ['https://<mediation_server>/publicapi/<org>/sites/2/']
}

requests.post('https://<mediation_server>/publicapi/<org>/accessprofiles/',
json=data, headers={"Authorization":id})
```

2.7.2 Groupes et domaines d'authentification

Les groupes d'utilisateurs associés aux différents contrats sont gérés par une URL spécifique qui inclut l'identifiant du contrat d'accès concerné.

URL : publicapi/<ORGANISATION>/accessprofiles/<ID>/groups/

Note : seules les méthodes « GET » et « PUT » sont acceptées pour cette URL. De plus, les modifications remplacent intégralement l'ancienne liste de groupes associés à un contrat d'accès par la nouvelle liste fournie.

Format des données :

```
{
    "name": "group_name",
    "domain": "https://<mediation_server>/publicapi/<org>/domains/<id>/"
}
```

Paramètre	Description
name	Nom du groupe
domain	Dans les données reçues dans la réponse à une requête GET, ce champ contient l'URL de l'API REST référençant le domaine auquel appartient le groupe. Quand ce paramètre est spécifié dans une requête PUT pour définir les groupes d'un contrat d'accès, ce paramètre doit contenir le nom du domaine tel qu'il est enregistré dans **cyber**elements Cleanroom (voir Domaines d'authentification, paramètre « name »)

Exemple de re-définition des groupes d'un contrat d'accès:

```
data = [
    {'name':'group_name_1','domain':'domain_name_1'},
    {'name':'group_name_2','domain':'domain_name_1'},
]

requests.post('https://<mediation_server>/publicapi/<org>/accessprofiles/<id>',
json=data, headers={"Authorization":id})
```

2.7.3 Limitations

Actuellement, il n’est pas possible de configurer des groupes génériques d’utilisateurs via l’API REST (groupes « Tout le monde », permettant à un contrat de concerner tous les groupes d’un domaine sans distinctions).

Il n’est pas non plus possible de manipuler les conditions d’accès, les restrictions d’applications, les alertes, les connexions réseaux et les éléments relatifs aux alias personnels. Tous ces éléments nécessitent la console d’administration.

2.8 Domaines d'authentification

2.8.1 Tous types de domaines

URL :

publicapi/<ORGANISATION>/domains/

publicapi/<ORGANISATION>/domains/<ID>/

publicapi/<ORGANISATION>/domainbyname/<NAME>/

Note : seule la méthode « GET » est acceptée pour ces URL.

Format des données :

```
{
    "domain_id": 1,
    "name": "local",
    "cascade_index": -1,
    "microsoft_domain": "",
    "description": "authentification locale",
    "deleteOldSession": false
}
```

Paramètre	Description
domain_id	Identifiant du domaine (lecture seule)
name	Nom du domaine. Doit être unique
cascade_index	Ordre de priorité du domaine dans l'authentification en cascade. Plus ce numéro est petit, plus le domaine est prioritaire. Si l'index est égal à -1, alors le domaine ne fait pas partie de l'authentification en cascade
microsoft_domain	Nom du domaine Microsoft que ce domaine représente dans **cyber**elements Cleanroom
description	Texte descriptif du contrat d'accès
deleteOldSession	Activation de la suppression automatique de la connexion au portail utilisateur la plus ancienne quand un utilisateur atteint son nombre maximum de connexions simultanées

Exemple de récupération des domaines :

```
requests.get('https://<mediation_server>/publicapi/<org>/domains/',
headers={"Authorization":id})
```

Contenu de la réponse :


```
[
    {
        "domain_id": 1,
        "name": "local",
        "cascade_index": -1,
        "microsoft_domain": "",
        "description": "authentification locale",
        "deleteOldSession": false
    },
    {
        "domain_id": 2,
        "name": "__guests__",
        "cascade_index": -1,
        "microsoft_domain": "",
        "description": "",
        "deleteOldSession": false
    },
    {
        "domain_id": 3,
        "name": "LDAP Dom 1",
        "cascade_index": -1,
        "microsoft_domain": "systancia.com",
        "description": "",
        "deleteOldSession": false
    }
]
```

2.8.2 Domaines locaux

Il n’est pas possible de manipuler les domaines locaux via l’API REST.

2.8.3 Domaines SAML

2.8.3.1 Gestion des domaines

URL :

publicapi/<ORGANISATION>/samldomains/

publicapi/<ORGANISATION>/samldomains/<ID>/

publicapi/<ORGANISATION>/samldomainbyname/<NAME>/

Format des données :

```
{
    "saml_domain_id": 1,
    "domain": {
        "domain_id": 5,
        "name": "test SAML domain",
        "cascade_index": -1,
        "microsoft_domain": "lan.local",
        "description": "",
        "deleteOldSession": false
    },
    "expiration_minutes": 10,
    "groups_attr": "group-attr",
    "user_attr": "user-attr",
    "email_attr": "",
    "max_connections": 10,
    "IDP": "other",
    "IDP_entityId": "entityId",
    "last_group_update_date": null
}
```

Paramètre	Description
saml_domain_id	Identifiant du domaine SAML (lecture seule). C'est cet identifiant qui doit être référencé dans l'URL des requêtes vers l'API REST ciblant un domaine SAML
domain	Objet contenant les paramètres de base du domaine. Le format des données de cet objet est celui spécifié dans la section Tous types de domaines
expiration_minutes	Délai d'expiration des sessions ouvertes par les utilisateurs appartenant au domaine SAML, en minutes
groups_attr	Nom de l'attribut de mappage SAML contenant le nom du groupe de l'utilisateur
user_attr	Nom de l'attribut de mappage SAML contenant le nom de l'utilisateur

email_attr	Nom de l'attribut de mappage SAML contenant l'adresse email de l'utilisateur. Paramètre inutilisé par **cyber**elements Cleanroom
max_connections	Nombre maximum de connexions simultanées autorisées pour ce domaine
IDP	Type de fournisseur d'identité du domaine SAML. Peut prendre la valeur « azure » ou « other »
IDP_entityId	*EntitiyID* du fournisseur d'identité du domaine SAML
last_group_update_date	Date de la dernière synchronisation des groupes Azure du domaine SAML (lecture seule). N'est mis à jour que pour les domaines SAML ayant un fournisseur d'identité *Azure*

Exemple de récupération des domaines SAML :

```
requests.get('https://<mediation_server>/publicapi/<org>/samldomains/',
headers={"Authorization":id})
```

Contenu de la réponse :

```
[
    {
        'saml_domain_id': 2,
        'domain': {'domain_id': 6, 'name': 'test Azure SAML domain',
'cascade_index': -1, 'microsoft_domain': 'lan.local', 'description': '',
'deleteOldSession': False},
        'expiration_minutes': 10,
        'groups_attr': 'group-attr',
        'user_attr': 'user-attr',
        'email_attr': '',
        'max_connections': 10,
        'IDP': 'azure',
        'IDP_entityId': 'https://sts.windows.net/ID/',
        'last_group_update_date': None
    },
    {
        'saml_domain_id': 1,
        'domain': {'domain_id': 5, 'name': 'test SAML domain', 'cascade_index': -
1, 'microsoft_domain': 'lan.local', 'description': '', 'deleteOldSession': False},
        'expiration_minutes': 10,
        'groups_attr': 'group-attr',
        'user_attr': 'user-attr',
        'email_attr': '',
        'max_connections': 10,
        'IDP': 'other',
        'IDP_entityId': 'entityId',
        'last_group_update_date': None
    }
]
```

Exemple de création de domaine SAML :

```
data = {
    'domain': {
        'name': 'test Azure SAML domain',
        'cascade_index': -1,
        'microsoft_domain': 'lan.local',
        'description': 'Created with REST API',
        'deleteOldSession': False
    },
    'expiration_minutes': 10,
    'groups_attr': 'group-attr',
    'user_attr': 'user-attr',
    'max_connections': 10,
    'IDP': 'azure',
    'IDP_entityId': 'https://sts.windows.net/ID/',
    'email_attr': ''
}

requests.post('https://<mediation_server>/publicapi/<org>/samldomains/',
json=data, headers={"Authorization":id})
```

Exemple de suppression de domaine SAML :

```
requests.delete('https://<mediation_server>/publicapi/<org>/samldomains/2/',
headers={"Authorization":id})
```

2.8.3.2 Gestion des groupes

URL :

publicapi/<ORGANISATION>/samldomains/<ID_DOMAIN>/groups/

publicapi/<ORGANISATION>/samldomains/<ID_DOMAIN>/groups/<ID_GROUP>/

Note : la seconde URL mentionnée ci-dessus ne supporte pas d'autres méthodes que DELETE.

Format des données :

```
{
    "group_id": 1,
    "name": "saml_grp1",
    "external_id": "saml_grp1_ext",
    "description": ""
}
```

Paramètre	Description
group_id	Identifiant du groupe SAML (lecture seule)
name	Nom du groupe SAML. Doit être unique au sein du domaine SAML
external_id	Identifiant externe du groupe SAML. Utilisé pour les domaines ayant un fournisseur d'identité Azure, où il doit être égal à l'identifiant du groupe au sein d'Azure
description	Texte descriptif du groupe SAML

Exemple de récupération des groupes d'un domaine SAML :

```
requests.get('https://<mediation_server>/publicapi/<org>/samldomains/1/groups/',
headers={"Authorization":id})
```

Contenu de la réponse :

```
[
    {'group_id': 1, 'name': 'saml_grp1', 'external_id': 'saml_grp1_ext',
'description': ''},
    {'group_id': 3, 'name': 'saml_grp2', 'external_id': 'saml_grp2_ext',
'description': ''}
]
```

Exemple de création d'un groupe :

```
data = {
    'name':'saml_grp3',
    'external_id': 'aaaaaaaa-aaaa-aaaa-aaaaaaaaaaaaaaaa',
    'description': 'Created through REST API'
}
requests.post('https://<mediation_server>/publicapi/<org>/samldomains/1/groups/',
json=data, headers={"Authorization":id})

Contenu de la réponse :
{
    'group_id': 7,
    'name': 'saml_grp3',
    'external_id': 'aaaaaaaa-aaaa-aaaa-aaaaaaaaaaaaaaaa',
    'description': 'Created through REST API'
}
```

Exemple de suppression d'un groupe :

```
requests.delete('https://<mediation_server>/publicapi/<org>/samldomains/1/groups/7
/', headers={"Authorization":id})
```

2.8.4 Groupes d'administrateurs

URL :

publicapi/<ORGANISATION>/admingroups/

publicapi/<ORGANISATION>/admingroups/<ID>/

Format des données :

```
{
    "admin_group_id": 1,
    "group": "admin group 1",
    "domain": "https://<mediation_server>/publicapi/<org>/domains/<id>",
    "delegated_administrators": false
}
```

Paramètre	Description
admin_group_id	Identifiant du groupe d'administrateur (lecture seule)
group	Nom du domaine à définir comme groupe d'administrateur
domain	Référence vers le domaine LDAP ou SAML auquel appartient le groupe, sous la forme d'une URL de l'API REST
delegated_administrators	Activation du mode *groupe d'administrateurs délégués*

Exemple de création de groupe d'administrateurs :

```
data = {
    'group':'ldap_grp_name',
    'domain':'https://<mediation_server>/publicapi/<org>/domains/3/',
    'delegated_administrators':False
}

requests.post('https://<mediation_server>/publicapi/<org>/admingroups/', json=data
headers={"Authorization":id})
```

Contenu de la réponse :

```
{
    'admin_group_id': 3,
    'group': 'ldap_grp_name',
    'domain':'https://<mediation_server>/publicapi/<org>/domains/3/',
    'delegated_administrators': False
}
```

Exemple de modification du nom de ce groupe d'administrateur :

```
data = {'group': 'ldap_grp_name modified'}

requests.patch('https://<mediation_server>/publicapi/<org>/admingroups/3/',
json=data headers={"Authorization":id})
```

Contenu de la réponse :

```
{
    'admin_group_id': 3,
    'group': 'ldap_grp_name modified',
    'domain': 'https://10.68.243.14/publicapi/<org>/domains/3/',
    'delegated_administrators': False
}
```

2.9 Coffre-fort

L'API REST permet uniquement la gestion des alias du coffre-fort. Elle ne permet pas la gestion des *alias dynamiques*, des *politiques de mot de passe*, des *comptes supervisés* et de l'*historique des expositions*.

De plus, l'API REST ne permet pas la gestion des alias lorsque le coffre-fort est en mode *Keeper*.

Enfin, il n'est ni possible de révéler le mot de passe d'un alias, ni possible de déclencher sa rotation via l'API REST.

2.9.1 Alias du coffre-fort

URL :

/publicapi/<ORGANISATION>/alias/

/publicapi/<ORGANISATION>/alias/<ID>/

/publicapi/<ORGANISATION>/aliasbyname/<NAME>/

Format des données :

```
{
    "id": 2,
    "name": "test_alias_name",
    "user_name": "ssh_user",
    "user_domain": "",
    "alias_type": 2,
    "policy": "DefaultPolicy",
    "password": ""
}
```

Paramètre	Description
id	Identifiant de l'alias (lecture seule)
name	Nom de l'alias. Doit être unique. Ne peut pas être modifié une fois l'alias créé
user_name	Login du compte représenté par l'alias
user_domain	Nom du domaine auquel le compte représenté par l'alias appartient. Pertinent uniquement si le paramètre « alias_type » vaut 3
alias_type	Type de l'alias. Peut prendre l'une des valeurs suivantes : • 1 : l'alias représente une clé SSH • 2 : l'alias représente un compte utilitateur SSH (sans domaine)

	• 3 : l'alias représente un compte utilisateur LDAP (avec domaine)
policy	Nom de la politique de mot de passe auquel l'alias appartient
password	Mot de passe ou clé SSH à enregistrer dans l'alias, en fonction du paramètre « alias_type » (écriture seule). Ce champ est obligatoire pour les créations de nouveaux alias. Dans le cas d'un alias de type 1, la clé SSH doit être la clé privée et doit être spécifiée au format texte, sans chiffrement

Exemple de création d'un alias :

```
data = {
    'name': 'test_alias_name',
    'user_name': 'test_username',
    'user_domain': '',
    'alias_type': 2,
    'policy': 'DefaultPolicy',
    'password': 'secret',
}

requests.post('https://<mediation_server>/publicapi/<org>/alias/', json=data,
headers={"Authorization": id})
```

Exemple de contenu de la réponse :

```
{'id': 8}
```

Exemple de récupération des données de cet alias :

```
requests.get('https://<mediation_server>/publicapi/<org>/alias/8/',
headers={"Authorization": id})
```

Contenu de la réponse :

```
{
    'id': 8,
    'name': 'test_alias_name',
    'user_name': 'test_username',
    'user_domain': '',
    'alias_type': 2,
    'policy': 'DefaultPolicy'
}
```

2.9.2 Alternatives

En plus de l'URL décrite précédemment, les alias du coffre-fort peuvent être manipulés via un certain nombre d'URL alternatives, mettant à profit une autre information que l'identifiant de l'alias.

URL alternatives :

/publicapi/<ORGANISATION>/aliasbyresourcename/<APPLICATIONNAME>/

/publicapi/<ORGANISATION>/aliasbylogin/<LOGINALIAS>/

Ces URL nécessitent obligatoirement une information supplémentaire, qui est utilisé à la place de l'identifiant de l'alias pour cibler ce dernier :

- « aliasbyresourcename » prend le nom de l'application à laquelle l'alias est associé (voir Paramètres communs, paramètre « name »)
- « aliasbylogin » prend le login du compte représenté par l'alias (voir Alias du coffre-fort, paramètre « user_name »)

Ces URL ont un fonctionnement similaire à l'URL /publicapi/<ORGANISATION>/alias/<ID>/, et ont notamment la même limitation en ce qui concerne les éventuels doublons : si l'information spécifiée ne permet pas de désigner un alias unique, la requête échouera avec une code http 500.

Il faut donc faire attention en utilisant ces alternatives, car elles se basent sur des informations qui peuvent naturellement mener à plusieurs alias :

- Pour « aliasbyresourcename », une application peut référencer plusieurs alias, menant à un échec.
- Pour « aliasbylogin », il est possible d'avoir plusieurs alias avec le même paramètre « user_name », menant là aussi à un échec. De plus, les paramètres « alias_type » et « user_domain » ne sont pas pris en compte pour ces requêtes.

3 API Console système

3.1 Authentification

Chaque appel à l'API nécessite d'être authentifié. L'authentification repose sur l'en-tête HTTP « Authorization », qui doit être spécifié dans toutes les requêtes vers l'API **cyber**elements Cleanroom. Cet en-tête doit contenir un jeton obtenu préalablement par un appel à une fonction dédiée à l'URL publicapi/su-api-auth.

Pour l'API de la console système, le nom d'utilisateur à spécifier est toujours « su », tandis que le mot de passe est celui servant à l'authentification sur la console système.

Exemple d'obtention du jeton :

```
import requests

r = requests.post('https://<mediation_server>/publicapi/su-api-auth', json={
    'login': 'su',
    'password': 'secret'
})
data = r.json()
try:
    id = data['id']
    print("Authentication succeeded")
except KeyError:
    print("Authentication failed")
    sys.exit(1)
```

L'appel doit contenir les paramètres suivants, en suivant la syntaxe JSON :

Paramètres	Description
login	Le nom du compte de l'administrateur système. Doit toujours valoir « su »
password	Le mot de passe de l'administrateur système

La réponse doit contenir un objet JSON contenant un champ « id » qui contient le jeton attendu. Ce jeton devra ensuite être placé dans l'en-tête « Authorization » pour les requêtes suivantes. Les exemples dans les sections suivantes incluront cet en-tête.

Si la réponse ne contient pas de champ « id », alors l'authentification a échoué.

3.2 Rechargement du service Apache

URL :

/publicapi/apache/reload/

Note : cette url n'accepte que des requêtes POST, sans contenu.

La modification d'éléments de la console système via cette API REST peut avoir un impact sur la configuration du service Apache des serveurs Mediation Controller. Aussi, la prise en compte des modifications peut nécessiter un rechargement du service, qui n'a pas lieu automatiquement.

Il est possible de manuellement déclencher cette opération depuis la console d'administration, en utilisant l'URL ci-dessus.

3.3 Organisations

URL :

/publicapi/organizations/

/publicapi/organizations/<ID_OR_NAME>/

/publicapi/organizations/<ID_OR_NAME>/delete/

Note : cette dernière URL accepte uniquement des requêtes POST, et est équivalente à une requête DELETE utilisant la seconde URL.

Les manipulations d'organisations acceptent des paramètres différents suivant si la requête vers l'API est une requête de création d'organisation ou non. Ci-dessous se trouve la structure des données de base, qui correspond à ce qui est attendu pour une modification (PUT ou PATCH) et à ce qui sera renvoyé comme réponse aux requêtes de lecture.

Format des données de base :

```
{
    "org_id": 1,
    "name": "organization_1",
    "admin_pwd": "",
    "allow_html5": true,
    "allow_acm": false,
    "su_organization_ip_set": [
        "1.1.1.1",
        "1.1.1.2",
        "1.1.1.3"
    ],
    "creation_state": "2",
    "safe_max_user": 5,
    "nb_max_sessions_user": 2
}
```

Paramètres	Description
org_id	Identifiant de l'organisation (lecture seule)
name	Nom de l'organisation
admin_pwd	Mot de passe de l'administrateur par défaut du domaine « *local* » de l'organisation (écriture seule)
allow_html5	Activation de l'autorisation des connexions HTML5 pour cette organisation, permettant l'utilisation d'Edge Gateway et d'applications HTML5
allow_acm	Activation de l'utilisation du *Application Credential Manager* (*ACM*) pour cette organisation
su_organization_ip_set	Liste des adresses IP autorisées à se connecter à la console d'administration de l'organisation (lecture seule)
creation_state	Etat actuel de l'organisation (lecture seule). Peut prendre l'une des valeurs suivantes : • « -1 » : Création imminente • « 0 » : Création interrompue à cause d'une erreur • « 1 » : En cours de création • « 2 » : Créée avec succès • « 3 » : En attente de connexion de l'Edge Gateway spécifiée *Note : bien que cet état soit représenté par un nombre entier, la valeur est transmise sous la forme d'une chaine de caractères*
safe_max_user	Nombre maximum de sessions utilisateurs
nb_max_sessions_user	Nombre maximum de sessions simultanées par utilisateur

Pour une création, un certain nombre de champs supplémentaires sont nécessaires, notamment ceux liés au serveur de base de données qui héberge ou hébergera la base d'organisation. Ces paramètres ne sont ensuite pas inclus dans les données reçues pour les requêtes GET, et ne sont pas éditables.

La création d'une organisation est une tâche asynchrone, et la requête de création recevra une réponse avant que l'organisation soit effectivement créée avec succès. Pour refléter ce fait, une requête de création reçoit un code de retour 202 « Accepted » en cas de succès, au lieu du code 201 « Created » habituel. De plus, cette réponse n'a aucun contenu. Une fois cette réponse reçue, l'avancement de la création peut être suivi via le paramètre « creation_state » qui inclut dans les données de l'organisation renvoyées en réponse aux requêtes GET.

Il n'est actuellement pas possible de spécifier une Edge Gateway à utiliser pour la création de l'organisation. Cette fonctionnalité n'est utilisable que via la console système **cyber**elements Cleanroom.

Format des données à transmettre pour une création uniquement :

```
{
    "name": "ipdivasafe",
    "db_login": "database_user",
    "db_pwd": "secret",
    "db_host": "127.0.0.1",
    "db_type": "PostgreSQL",
    "db_ssl_mode": "verify-full",
    "db_pkiid": "1750162818913",
    "db_caid": "2411074302",
    "admin_pwd": "secret2",
    "db_port": 5432,
    "allow_html5": true,
    "allow_acm": true,
    "su_organization_ip_set": ["1.1.1.1", "1.1.1.2", "1.1.1.3"],
    "create_database": true,
    "safe_max_user": 5,
    "nb_max_sessions_user": 2
}
```

Paramètres	Description
name	Nom de l'organisation
db_login	Nom du compte à utiliser pour accéder à la base de données de l'organisation
db_pwd	Mot de passe du compte à utiliser pour accéder à la base de données de l'organisation
db_host	Adresse du serveur hébergeant la base de données de l'organisation
db_type	Type de serveur de base de données. Peut valoir « PostgreSQL » ou « Microsoft SQL Server »
db_ssl_mode	Politique d'utilisation de SSL. Peut prendre l'une des valeurs suivantes : • « prefer » : Privilégier SSL sans vérifier le certificat (non-sécurisé) • « verify-ca » : Vérifier le certificat du serveur • « verify-full » : Vérifier le certificat du serveur et son nom
db_pkiid	Identifiant de la PKI à utiliser (Voir PKI, paramètre « id »). Pertinent uniquement si le paramètre « db_ssl_mode » est défini à « verify-ca » ou « verify-full »
db_caid	Identifiant de l'autorité de certification de la PKI à utiliser (Voir Autorités de certification, paramètre « id »). Pertinent

	uniquement si le paramètre « db_ssl_mode » est défini à « verify-ca » ou « verify-full »
admin_pwd	Mot de passe de l'administrateur par défaut du domaine « *local* » de l'organisation
db_port	Port à utiliser pour les communications avec la base de données de l'organisation
allow_html5	Activation de l'autorisation des connexions HTML5, permettant l'utilisation d'Edge Gateways et d'applications HTML5
allow_acm	Activation de l'utilisation du *Application Credential Manager* (*ACM*) pour cette organisation
create_database	Activation de la création de base de données. Si cette option est activée, la base de données de l'organisation sera automatiquement créée sur le serveur de base de données spécifié. Si elle est désactivée, la base d'organisation doit déjà exister
su_organization_ip_set	Liste des adresses IP autorisées à se connecter à la console d'administration de l'organisation
safe_max_user	Nombre maximum de sessions utilisateurs
nb_max_sessions_user	Nombre maximum de sessions simultanées par utilisateur

Exemple de création :

```
data = {
    'name': 'dummy_2',
    'db_login': 'database_user',
    'db_pwd': 'secret',
    'db_host': '127.0.0.1',
    'db_type': 'PostgreSQL',
    'db_ssl_mode': 'prefer',
    'admin_pwd': 'secret2',
    'db_port': 5432,
    'allow_html5': True,
    'allow_acm': True,
    'create_database': False,
    'safe_max_user': 10,
    'nb_max_sessions_user': 1,
    'su_organization_ip_set': ['1.1.1.1', '1.1.1.2', '1.1.1.3']
}

requests.post('https://<mediation_server>/publicapi/organizations/', json=data,
headers={"Authorization": id})
```

Exemple de vérification de l'état d'avancement de la création de l'organisation :

```
response = requests.get('https://<mediation_server>/publicapi/organizations/4/',
headers={"Authorization": id})
try:
    creation_state = response.json()['creation_state']

    creation_ongoing = creation_state in ['-1', '1', '3']
    created_successful = creation_state == '2'
    creation_failed = creation_state == '0'
except requests.exceptions.JSONDecodeError | KeyError:
    # Requête échouée
    pass
```

3.4 PKI et données associées

3.4.1 Public Key Infrastructure (PKI)

URL :

/publicapi/pki/

/publicapi/pki/<NAME>/

Note : il n'est pas possible de créer, modifier ou supprimer des PKI via l'API REST. Seules les requêtes GET sont acceptées. Tous les paramètres présentés ci-dessous sont donc en lecture seule.

Format des données :

```
{
    "name": "PKI name",
    "description": "",
    "usage": "ABC",
    "active": false,
    "id": "pki_id",
    "casDir": "/etc/ipdiva/pkis/pki_id/ca",
    "hasCa": true,
    "hasCert": true
}
```

Paramètres	Description
name	Nom de la PKI. Doit être unique
description	Texte descriptif de la PKI
usage	Mode d'utilisation de la PKI. Peut prendre l'une des valeurs suivantes : • « A » : Certificats pour les serveurs web • « B » : Certificats pour l'authentification des utilisateurs • « C » : Certificats pour les Edge Gateways/serveurs Mediation Controller • « AB » : Certificats pour les serveurs web et l'authentification des utilisateurs • « AC » : Certificats pour les serveurs web et les Edge Gateways/serveurs Mediation Controller • « BC » : Certificats pour les Edge Gateways/serveurs Mediation Controller et l'authentification des utilisateurs • « ABC » : Certificats pour les serveurs web et l'authentification des utilisateurs et les Edge Gateways/serveurs Mediation Controller

active	Paramètre inutilisé
id	Identifiant unique de la PKI
casDir	Chemin vers l'emplacement, sur le serveur Mediation Controller, des données liées aux autorités de certification de cette PKI.
hasCa	Indicateur précisant si la PKI a au moins une autorité de certification configurée
hasCert	Indicateur précisant si au moins l'une des autorités de certification configurées pour cette PKI a un certificat

Exemple de récupération d'une PKI nommée « PKI test » :

```
requests.get('https://<mediation_server>/publicapi/pki/PKI test/',
headers={"Authorization": id})
```

Contenu de la réponse :

```
{
    'name': 'PKI test',
    'description': '',
    'usage': 'ABC',
    'active': False,
    'id': '1750162818913',
    'casDir': '/etc/ipdiva/pkis/1750162818913/ca',
    'hasCa': True,
    'hasCert': True
}
```

3.4.2 Autorités de certification (CA)

URL :

/publicapi/pki/<PKI_NAME>/ca/

/publicapi/pki/<PKI_NAME>/ca/<CA_NAME>/

Note : il n'est pas possible de créer, modifier ou supprimer des autorités de certification via l'API REST. Seules les requêtes GET sont acceptées. Tous les paramètres présentés ci-dessous sont donc en lecture seule.

Format des données :

```
{
    "name": "CA-NAME",
    "id": "id",
    "isRootCA": true,
    "subject": "/CN=CA-NAME",
    "issuer": "/CN=CA-NAME",
    "certFilePath": "/etc/ipdiva/pkis/pki_id/ca/id.pem",
    "hasCert": true
}
```

Paramètres	Description
name	Nom de l'autorité de certification
id	Identifiant de l'autorité de certification
isRootCA	Indicateur précisant si l'autorité de certification est une autorité *racine*
subject	Sujet du certificat de l'autorité de certification
issuer	Emetteur du certificat de l'autorité de certification
certFilePath	Chemin vers l'emplacement, sur le serveur Mediation Controller, du fichier du certificat de l'autorité de certification
hasCert	Indicateur précisant si l'autorité de certification a au moins un certificat enregistré

Exemple de récupération des autorités de certifications d'une PKI « PKI test » :

```
requests.get('https://<mediation_server>/publicapi/pki/PKI test/ca/',
headers={"Authorization": id})
```

Contenu de la réponse :

```
[
    {
        'name': 'TEST-CA',
        'id': '2411074302',
        'isRootCA': True,
        'subject': '/CN=TEST-CA',
        'issuer': '/CN=TEST-CA',
        'certFilePath': '/etc/ipdiva/pkis/1750162818913/ca/2411074302.pem',
        'hasCert': True
    }
]
```

3.4.3 Certificats des autorités de certifications

URL :

/publicapi/pki/<PKI_NAME>/ca/<CA_NAME>/cert/

/publicapi/pki/<PKI_NAME>/ca/<CA_NAME>/cert/<CERT_NAME>/

Note : il n'est pas possible de créer, modifier ou supprimer des certificats d'autorités de certification via l'API REST. Seules les requêtes GET sont acceptées. Tous les paramètres présentés ci-dessous sont donc en lecture seule.

Format des données :

```
{
    "name": "cert_name",
    "id": "cert_id",
    "subject": "/CN=subject",
    "issuer": "/CN=issuer",
    "notBefore": "2023-01-01 00:00:01",
    "notAfter": "2025-01-01 00:00:01",
    "certFilePath": "/etc/ipdiva/pkis/pki_id/ca/ca_id/cert_id.crt",
    "keyFilePath": "/etc/ipdiva/pkis/pki_id/ca/ca_id/cert_id.key",
    "kind": {
        "client": false,
        "clientCa": false,
        "server": false,
        "serverCa": false
    }
}
```

Paramètres	Description
name	Nom du certificat
id	Identifiant interne pour le certificat
subject	Sujet du certificat
issuer	Emetteur du certificat
notBefore	Date de début de validité du certificat
notAfter	Date de fin de validité du certificat
certFilePath	Chemin vers l'emplacement, sur le serveur Mediation Controller, du fichier de certificat signé
keyFilePath	Chemin vers l'emplacement, sur le serveur Mediation Controller, du fichier contenant la clé privée du certificat

kind	Objet contenant des informations à propos des utilisations possibles pour ce certificat, en accord avec les extensions définies dans le certificat.

Exemple de récupération de la liste des certificats enregistrés pour une autorité de certification « TEST-CA » associé à une PKI « PKI test » :

```
requests.get('https://<mediation_server>/publicapi/pki/PKI test/ca/TEST-CA/cert/',
headers={"Authorization": id})
```

Contenu de la réponse :

```
[
        {
            'name': '*.lan.local',
            'id': '2628909733',
            'subject': '/CN=*.lan.local',
            'issuer': '/CN=TEST-CA',
            'notBefore': '2025-04-10 09:15:19',
            'notAfter': '2027-04-10 09:15:19',
            'certFilePath':
'/etc/ipdiva/pkis/1750162818913/ca/2411074302/2628909733.crt',
            'keyFilePath':
'/etc/ipdiva/pkis/1750162818913/ca/2411074302/2628909733.key',
            'kind': {'client': False, 'clientCa': False, 'server': True,
'serverCa': False}
        }
]
```

3.5 Hôtes virtuels

URL :

/publicapi/virtualhosts/

/publicapi/virtualhosts/<ID>/

/publicapi/virtualhostsbyname/<NAME>/

Ces URL permettent de lister tous les hôtes virtuels configurés, indépendamment de leurs types respectifs. Cependant, en fonction de ces types, les données des hôtes virtuels changent.

3.5.1 Données communes

Les hôtes virtuels ont un certain nombre de paramètres communs, indépendamment de leurs types.

Format des données communes :


```
{
    "name": "test_virtualhost",
    "domainName": "local",
    "adminMail": "admin@lan.local",
    "specificSSLCert": false,
    "SSLConfigOverride": {},
    "SSLUserAuthConfig": false,
    "SSLUserAuthConfigOverride": {},
    "type": "type",
    "id": "test_virtualhost",
    "forInterface": "type : test_virtualhost"
}
```


Paramètres	Description
name	Nom de l'hôte virtuel *Note : Il est déconseillé de spécifier un nom contenant un ou plusieurs espaces*
domainName	Nom du domaine sur lequel l'hôte virtuel doit s'appliquer
adminMail	Adresse email de l'administrateur
specificSSLCert	Paramètre inutilisé
SSLConfigOverride	Paramètre inutilisé

SSLUserAuthConfig	Paramètre inutilisé
SSLUserAuthConfigOverride	Paramètre inutilisé
type	Type de l'hôte virtuel. Peut prendre l'une des valeurs suivantes : • « webvpn » pour un hôte virtuel *Web VPN* • « reverseproxy » pour un hôte virtuel *Reverse Proxy* • « transparentreverseproxy » pour un hôte virtuel *Reverse Proxy Transparent*
id	Identifiant de l'hôte virtuel (lecture seule). Egal au nom que l'hôte virtuel avait lors de sa création
forInterface	Paramètre inutilisé

Exemple de récupération des hôtes virtuels :

```
requests.get('https://<mediation_server>/publicapi/virtualhosts/',
headers={"Authorization": id})
```

Contenu de la réponse :

```
[
    {
        'name': 'default',
        'domainName': '',
        'adminMail': 'support@ipdiva.com',
        'specificSSLCert': False,
        'SSLConfigOverride': {},
        'SSLUserAuthConfig': False,
        'SSLUserAuthConfigOverride': {},
        'publishPortal': True,
        'baseRedirection': '/gate/cloud/',
        'HTTPRedirect': False,
        'HTTPRedirectDomains': [],
        'enableActiveSync': True,
        'orgActiveSync': '',
        'enableCARE': True,
        'enableShibboleth': False,
        'enableCyberelements': False,
        'filterOrgs': False,
        'filterOrgList': [],
        'setCybeltOrg': '',
        'type': 'webvpn',
        'id': 'default',
        'forInterface': 'webvpn : default'
    },
    {
        'name': 'Test_RP',
        'domainName': 'lan.local',
```

```
        'adminMail': 'admin@lan.local',
        'specificSSLCert': False,
        'SSLConfigOverride': {},
        'SSLUserAuthConfig': False,
        'SSLUserAuthConfigOverride': {},
        'authenticationRedirect': 'auth_redirection.lan.local',
        'type': 'reverseproxy',
        'id': 'Test_RP',
        'forInterface': 'reverseproxy : Test_RP'
    },
    {
        'name': 'Test_RP_Transparent',
        'domainName': 'lan.local',
        'adminMail': 'admin@lan.local',
        'specificSSLCert': False,
        'SSLConfigOverride': {},
        'SSLUserAuthConfig': False,
        'SSLUserAuthConfigOverride': {},
        'orgTransparentRP': 'organization01',
        'targetTransparentRP': 'target.lan.local',
        'protocolTransparentRP': 'https',
        'siteTransparentRP': '1',
        'activeGatewaysTransparentRP': ['test gateway'],
        'passiveGatewaysTransparentRP': [],
        'cacheTransparentRP': True,
        'preserveHostTransparentRP': False,
        'redirectionsTransparentRP': [],
        'ntlmConfig': False,
        'mappingTransparentRP': [],
        'type': 'transparentreverseproxy',
        'id': 'Test_RP_Transparent',
        'forInterface': 'transparentreverseproxy : Test_RP_Transparent'
    }
]
```

3.5.2 Données des hôtes virtuels Web VPN

Format des données :

```
{
    "publishPortal": true,
    "baseRedirection": "",
    "HTTPRedirect": false,
    "HTTPRedirectDomains": [
        ""
    ],
    "enableActiveSync": false,
    "orgActiveSync": "",
    "enableCARE": true,
    "enableShibboleth": false,
    "enableCyberelements": false,
    "filterOrgs": false,
    "filterOrgList": [],
    "setCybeltOrg": ""
}
```

Paramètres	Description
publishPortal	Activation de la publication du portail **cyber**elements Cleanroom avec cet hôte virtuel
baseRedirection	Redirection d'URL de base, utilisée quand un utilisateur tente d'accéder à la racine de l'hôte virtuel
HTTPRedirect	Activation de la redirection HTTP, redirigeant automatiquement les utilisateurs vers l'interface HTTPS s'ils tentent d'accéder à l'interface HTTP
HTTPRedirectDomains	Liste des noms de domaines devant être soumis à la redirection HTTP. Pertinent uniquement si l'option « HTTPRedirect » est activée
enableActiveSync	Paramètre inutilisé
orgActiveSync	Paramètre inutilisé
enableCARE	Paramètre inutilisé
enableShibboleth	Activation du module SAML de **cyber**elements Cleanroom, reposant sur *Shibboleth*
enableCyberelements	Paramètre inutilisé
filterOrgs	Paramètre inutilisé

filterOrgList	Paramètre inutilisé
setCybeltOrg	Paramètre inutilisé

3.5.3 Données des hôtes virtuels Reverse Proxy

Format des données :

```
{
    "authenticationRedirect": "auth_redirection.lan.local"
}
```

Paramètres	Description
authenticationRedirect	Nom de l'hôte vers lequel les utilisateurs doivent être redirigés pour l'authentification s'ils ne sont pas déjà authentifiés

3.5.4 Données des hôtes virtuels Reverse Proxy Transparent

Format des données :

```
{
    "orgTransparentRP": "organization01",
    "targetTransparentRP": "target.lan.local",
    "protocolTransparentRP": "https",
    "siteTransparentRP": "site_id ",
    "activeGatewaysTransparentRP": [
        "test gateway"
    ],
    "passiveGatewaysTransparentRP": [],
    "cacheTransparentRP": true,
    "preserveHostTransparentRP": false,
    "redirectionsTransparentRP": [],
    "ntlmConfig": false,
    "mappingTransparentRP": []
}
```

Paramètres	Description
orgTransparentRP	Nom de l'organisation **cyber**elements Cleanroom contenant le site à utiliser pour joindre le service cible
targetTransparentRP	Service ciblé par le reverse proxy transparent
protocolTransparentRP	Protocole à utiliser pour atteindre le service cible. Peut valoir « http » ou « https »
siteTransparentRP	Identifiant du site à utiliser pour joindre le service cible. Doit faire partie de l'organisation nommée dans le paramètre « orgTransparentRP » *Note : bien que cet identifiant soit un nombre entier, le paramètre doit être une chaine de caractère représentant ce nombre*
activeGatewaysTransparentRP	Liste des noms d'Edge Gateways actives du site spécifié dans le paramètre « siteTransparentRP » (lecture seule)
passiveGatewaysTransparentRP	Liste des noms d'Edge Gateways passives du site spécifié dans le paramètre « siteTransparentRP » (lecture seule)
cacheTransparentRP	Activation du cache HTTP d'*Apache* sur le serveur de Mediation Controller
preserveHostTransparentRP	Paramètre inutilisé

redirectionsTransparentRP	Paramètre inutilisé
ntlmConfig	Paramètre inutilisé
mappingTransparentRP	Paramètre inutilisé

3.6 Interfaces Web

URL :

/publicapi/webinterfaces/

/publicapi/webinterfaces/<NAME>/

Format des données :

```
{
    "name": "default",
    "authType": "none",
    "crls": [""],
    "verifyDepth": 2,
    "certId": "",
    "pkiSelectId": "pki_id",
    "caSelectId": "ca_id",
    "certSelectId": "cert_id",
    "authCaIds": [
        "ca_id@pki_id",
        "ca_id@pki_id"
   ],
    "crlIds": [""],
    "enableOCSPStapling": false,
    "vhs": [
        ["default", true]
    ],
    "hostIds": ["standalone"],
    "webInterfaceId": "<ip_address>:<port>",
    "addressId": ""
}
```

Paramètres	Description
name	Nom de l'interface web (lecture seule). Doit être unique. Pour les interfaces Web autre que *default*, ce nom équivaut à l'adresse et le port de l'interface.
authType	Mode de gestion de l'authentification par certificat. Peut prendre l'une des valeurs suivantes : • « none » pour la désactiver • « optional » pour qu'elle soit optionnelle • « require » pour qu'elle soit obligatoire
crls	Paramètre inutilisé
verifyDepth	Profondeur de vérification des certificats
certId	Paramètre inutilisé

pkiSelectId	Identifiant de la PKI configurée pour cette interface Web (voir Public Key Infrastructure (PKI), paramètre « id »)
caSelectId	Identifiant de l'autorité de certification configurée pour cette interface Web (voir Autorités de certification (CA), paramètre « id »). Cette autorité doit faire partie de la PKI indiquée via le paramètre « pkiSelectId »
certSelectId	Identifiant du certificat configuré pour cette interface Web (voir Certificats des autorités de certifications, paramètre « id »). Ce certificat doit faire partie de l'autorité de certification indiquée via le paramètre « caSelectId »
authCaIds	Liste des autorités de certifications autorisées à émettre des certificats utilisateurs. Chaque élément de cette liste représente une autorité de certification sous la forme d'une chaine de caractères suivant la syntaxe suivante : « ca_id@pki_id »
crlIds	Paramètre inutilisé
enableOCSPStapling	Paramètre inutilisé
vhs	Liste des hôtes virtuels associés à cette interface Web. Chaque élément de cette liste représente un hôte virtuel, sous la forme d'une liste donnant le nom de ce dernier ainsi que son état « activé »
hostIds	Liste des serveurs Mediation Controller concernés par l'interface Web. En mode *standalone*, doit toujours contenir une seule valeur « standalone ». En mode *cluster* : • Si l'adresse de l'interface Web est l'adresse réelle de l'un des serveurs, *master* ou *slave*, cette liste doit contenir une seule valeur, respectivement « master » ou « slave » • Sinon, cette liste peut contenir l'une ou l'autre de ces valeurs ou bien les deux
webInterfaceId	Adresse et port de l'interface Web (création uniquement, écriture seule). Doit être unique. La valeur doit respecter la syntaxe « <ip_address>:<port> ». Une fois l'interface Web créée, le paramètre « name » de cette dernière contiendra la valeur spécifiée dans ce champ

addressId	Indicateur précisant si l'adresse de l'interface Web est particulière. Peut prendre l'une des valeurs suivantes : • « webRip » si l'adresse correspond à l'adresse IP réelle du serveur Mediation Controller *master* ou *slave* • « webVip » si l'adresse correspond à l'adresse IP virtuelle du *cluster* • « » (chaine vide) pour tous les autres cas, c'est-à-dire pour une installation *standalone* ou pour une adresse personnalisée sur une installation *cluster*

```
Exemple de création d'interface Web :
data = {
    "webInterfaceId": "<mediation_server>:8443",
    "authType": "none",
    "crls": [""],
    "verifyDepth": 2,
    "certId": "",
    "pkiSelectId": "1750162818913",
    "caSelectId": "2411074302",
    "certSelectId": "2628909733",
    "authCaIds": [""],
    "crlIds": [""],
    "enableOCSPStapling": false,
    "vhs": [
        ["default", true]
    ],
    "hostIds": ["standalone"],
    "addressId": ""
}

requests.post('https://<mediation_server>/publicapi/webinterfaces/',
json=data, headers={"Authorization": id})
```

SYSTANCIA

Actipolis 3, Bât C11

3, rue Paul Henri Spaak

68 390 SAUSHEIM

France

Téléphone : 03 89 33 58 20

Fax : 03 89 33 58 21

site web : https://www.sep.systancia.com